Belmont Law Review

Volume 5 *Symposium 2017: Education Reform at the Intersection of Law, Politics, and Policy*

Article 13

2018

Katz-Calls: Application of Fourth Amendment Protection to Police Use of Smartphone Emergency Functionality

Ryan Russell
Belmont University - College of Law

KATZ-CALLS: APPLICATION OF FOURTH AMENDMENT PROTECTION TO POLICE USE OF SMARTPHONE EMERGENCY FUNCTIONALITY

RYAN RUSSELL*

INTRODUCTION

It is estimated that sixty-eight percent of adults in the United States own and use a smartphone.[1] These devices have brought with them incredible efficiency and convenience, but those benefits are not without new complications. Seemingly ever more at the forefront of both political and

* Ryan Russell is a former music industry professional pursuing his Juris Doctor at Belmont University College of Law. He received his B.B.A. from Belmont University with a major in Music Business. Ryan and his wife, Susan, are members of Fellowship Bible Church in Brentwood, TN. They live in Nashville, where they enjoy camping, hiking, and pretty much anything else involving the outdoors.

1. Monica Anderson, *Technology Device Ownership: 2015*, PEW RES. CTR. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

technological debate is the concern of individual privacy, and the extent to which the government may intrude upon that privacy.

A novel legal question has been sparked by the existence of an emergency function ("Emergency") built into smartphones which allows a person, without knowing or contravening the phone's passcode, to make a call to any number. The Emergency button shows on the phone's lock screen and, when pressed, provides access, not only to a user's pre-loaded Medical ID information, but also to a dialing screen to be used for calling 911. The primary purpose of Emergency is safety—should a smartphone's user be incapacitated for any reason, a bystander can pick up that person's phone and get in touch with emergency services, regardless of whether the user locks their phone with a passcode.

While there are many obvious safety benefits to this technology, the ability to dial out from the phone in this way raises new legal issues. Particularly, would police use of the Emergency function on a lawfully-seized smartphone qualify as a search for purposes of the Fourth Amendment? Should officers be required to secure a warrant before being able to use the functionality in pursuit of a criminal suspect?

This issue was recently raised in a California court during a criminal case against Matthew Muller, who was on trial for burglarizing a home.[2] Allegedly, Muller was stealing from the home when he was confronted by the homeowner and fled, but not before dropping his iPhone.[3] Police recovered the phone and used the Emergency function to call 911—inherently giving the number associated with the phone to the 911 operator.[4] Officers got the phone number from 911 and determined the service provider.[5] At this point, they obtained a warrant, allowing police to get Muller's identification from the provider.[6]

At trial, Muller argued that the evidence obtained from the phone should be excluded because police use of the Emergency function was an illegal search.[7] Ultimately, this issue was not decided. The judge determined that the phone in this particular case was abandoned property, and therefore Muller had no privacy interest in it.[8] The question remains as to whether this

---

2. Orin Kerr, *Applying the Fourth Amendment to Placing Calls from a Locked Phone to Identify its Owner*, THE VOLOKH CONSPIRACY (June 22, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/22/applying-the-fourth-amendment-to-placing-calls-from-a-locked-phone-to-identify-its-owner/?utm_term=.6746bfbc9851.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. Rina Nakano, *Judge Rules Cell Phone Will Remain as Evidence in Kidnapping Case Against Matthew Muller*, FOX 40 (June 23, 2016, 4:22 PM), http://fox40.com/2016/06/23/judge-rules-cell-phone-will-remain-as-evidence-in-kidnapping-case-against-matthew-muller/.

could constitute a search under the Fourth Amendment under a different set of circumstances, however.

In determining whether an officer's use of the Emergency function of a phone is a search, it is important first to lay a foundation for why the Constitution provides protection against searches in the first place. Part I of this Note will provide a brief overview of why the Fourth Amendment was adopted, and what rights it is intended to protect. Next, it is impossible to know whether use of Emergency would qualify as a search unless we know how a search is defined. Part II of this Note will examine the tests that have developed over the years, namely the *Katz* test and the *Jones* test, which give the prevailing framework for determining whether a search has taken place. Part III will show how these tests have been adapted and made applicable to modern technology in our digital age. Technology has presented courts with a variety of legal issues to sort through and, though the question of Emergency use has not been settled at a circuit court level, related issues have already found their way into appellate jurisdiction. In Part IV, this Note will give a summation of what have come to be called the "MagStripe" cases, and will show how the legal questions at issue in those cases could come to bear heavily on the fate of Emergency use in future prosecutions. To conclude, Part V will address how the culmination of the case law indicates that police use of Emergency is not a search under the Fourth Amendment.

I. FOURTH AMENDMENT ORIGINS

An analysis of whether a police officer's use of the Emergency function on a smartphone constitutes a search cannot be undertaken without first obtaining an understanding of why the Constitution protects against searches, and what kind of rights and interests are included under this protection.

The Constitution provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[9] The origins of the Fourth Amendment "grew directly out of the events which immediately preceded the revolutionary struggle with England."[10] King Henry VIII had combined the government's power to search along with a licensing system to constrain the freedom of the press in England.[11] This arose from the publication of articles "attacking not only governmental policies but the King himself."[12] It was not until later in the 1600's that the English people began adopting the belief that "the public

9. U.S. CONST. amend. IV.

10. WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1(a) (5th ed. Supp. 2016).

11. *Id.*

12. Meghan Totten, *Constitution of the United States of America: Analysis, and Interpretation – Centennial Edition*, UNITED STATES GOVERNMENT PUBLISHING OFFICE, 1377-78 (June 27, 2016), https://www.congress.gov/content/conan/pdf/GPO-CONAN-REV-2016.pdf.

had a right to be safeguarded" from this kind of activity.[13] Professor LaFave[14] notes the words of William Pitt which summarize the heart of this movement:

> The poorest man may, in his cottage, bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.[15]

For colonials in particular, the Fourth Amendment represented "protection against the use of the 'writs of assistance.'"[16] These writs were issued by the Crown allowing officers to enter a premises and search for goods that may have been smuggled into the colonies.[17] Opposition to the writs was led by James Otis, whose unsuccessful attempts to defeat the writs paved the way for James Madison, who proposed that a clause nearly identical to the finalized Fourth Amendment be included in the Constitution.[18]

Now that we have a background for *why* the Fourth Amendment was enacted, *what* exactly was it meant to protect against? Simply put, it is a barrier, a hurdle that must be overcome before a government actor may intrude upon certain enumerated areas of individual privacy—the aforementioned "persons, houses, papers, and effects."[19] Generally speaking, that is going to include your smartphone, and more importantly, the data contained within your smartphone.

What kind of hurdle is created? Courts have held that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[20] More specifically, within the context of a search, "reasonableness" is typically going to require obtaining a warrant.[21] Warrants naturally slow down an officer's investigative process, but that is a price the judicial system is willing to pay in order to uphold the privacy interests recognized in the Constitution. The value of a warrant is its insertion of "the judgment of an independent magistrate between law enforcement officers and the privacy of citizens."[22] Unlike early seventeenth-century England, the Constitution places such importance on the individual right to privacy (though the extent is yet to be

13. LaFave, *supra* note 10, § 1.1(a) (quoting Nelson B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution*, 38-39 (1937)).

14. Professor Wayne LaFave is the author of the treatise *Search and Seizure*, and is a noted scholar on the Fourth Amendment.

15. *Id.* (quoting Nelson B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution*, 49-50 (1937)).

16. Totten, *supra* note 12, at 1378.

17. *Id.*

18. LaFave, *supra* note 10, § 1.1(a).

19. U.S. CONST. amend. IV.

20. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

21. Riley v. California, 134 S. Ct. 2473, 2482 (2014).

22. Totten, *supra* note 12 at 1399.

fully determined) that it is willing to impede public investigation, and consequently the search for truth, in an aim to uphold that privacy.

There are, however, circumstances in which our justice system has determined that the warrant requirement can be circumvented. A balancing test is applied in which courts "determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[23] Examples of legitimate governmental interests include officer safety and avoiding the loss or destruction of evidence.[24] To the extent there is a threat to officer safety or evidence, the warrant requirement is less likely to be waived.

The Fourth Amendment was enacted to protect the privacy of individuals and their possessions. This protection extends to smartphones and the data contained therein. And the protection is triggered any time a government actor conducts a search of that smartphone. In our hypothetical situation in which an officer uses the Emergency function of a suspect's smartphone without a warrant, three of the main requirements for a Fourth Amendment violation are clearly met. We have a government actor (police officer) and a protected piece of personal property (a smartphone). Furthermore, no warrant has been obtained by the government actor. The only remaining question is whether there has been a search. How do we know when a search has been conducted?

II. DEFINING A "SEARCH"

This section will summarize how courts have come to define a search for purposes of the Fourth Amendment. Traditionally, searches were heavily tied to physical trespass theory, but modern courts have adopted a more expansive view. Two cases in particular establish the framework under which a particular government action must be scrutinized to determine if there has been a search—*Katz v. United States*[25] and *United States v. Jones*[26]. *Katz* was decided in 1967, and there have been many cases since then that apply and interpret its holding and test. *Jones*, on the other hand, was decided in 2012, and the extent of its impact remains to be seen.

A search is broadly defined as "an infringement of an expectation of privacy that society is prepared to consider reasonable."[27] A search can take many different forms, but it will typically involve some exertion of force, whether large or small.[28] It includes "some exploratory investigation, . . . a

23. *Riley*, 134 S. Ct. at 2484.
24. *Id.* at 2485.
25. *See* 389 U.S. 347 (1967).
26. *See* 565 U.S. 400 (2012).
27. 79 C.J.S. Searches § 6 (2016). *See also Katz* 389 U.S. 347 (1967).
28. LaFave, *supra* note 10, § 2.1(a).

looking for or seeking out."[29] In contrast, "a truly cursory inspection—one that involves merely looking at what is already exposed to view, without disturbing it—is not a 'search' for Fourth Amendment purposes."[30] Additionally, because the Fourth Amendment protection "extends to governmental action only," courts have held that "once an individual's expectation of privacy in particular information has been frustrated by a private individual, the Fourth Amendment does not prohibit law enforcement's subsequent use of that information, even if obtained without a warrant."[31]

A. Katz v. United States

The first of the tests that is applied to determine whether a particular police action constitutes a search is the *Katz* test. Prior to *Katz*, a lack of physical penetration into someone's privacy was dispositive in determining that a search had not taken place.[32] However, courts began to take the view that "the Fourth Amendment protects people, not places," and therefore a search could potentially take place without physical intrusion.[33]

In *Katz*, the defendant was charged with conducting an interstate gambling business via telephone.[34] He was apprehended when FBI agents "attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls."[35] The lower courts ruled that there was no search, because the agents had not physically intruded upon the phone booth.[36]

The United States Supreme Court reversed, saying, "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[37] The court went further by saying, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what

29. *Id.*

30. Arizona v. Hicks, 480 U.S. 321, 328 (1987) (holding that "the distinction between 'looking' at a suspicious object in plain view and 'moving it even a few inches' is much more than trivial for purposes of the Fourth Amendment").

31. United States v. Sparks, 806 F.3d 1323, 1334 (11th Cir. 2015) (holding that the unwarranted search of a cell phone did not violate Fourth Amendment protections because the phone was found, unlocked, at a Walmart, and the police search of the phone did not extend beyond that conducted by private citizens who found the phone).

32. *Katz*, 389 U.S. at 352.

33. *Id.* at 351.

34. *Id.* at 348.

35. *Id.*

36. *Id.* at 348-49.

37. *Id.* at 353.

he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[38]

It is from this principle that Justice Harlan, in his concurrence, iterated what has come to be known as the *Katz* test. Harlan's concurrence is notable because "lower courts attempting to interpret and apply *Katz* quickly came to rely upon the Harlan elaboration, as ultimately did a majority of the Supreme Court."[39] Harlan noted that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[40]

The first prong of the test is somewhat problematic to enforce, as the Court takes the opportunity to dispose of previous standards without giving much substance to what the new standard actually is.[41] It has been noted that the requirement of an actual expectation of privacy in the first prong opens the requirement up to being manipulated.[42] "[T]he government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance."[43] As such, courts have warned that the first prong of the *Katz* test can provide an "inadequate index of Fourth Amendment protection."[44] Justice Harlan was satisfied that the defendant in *Katz* had fulfilled this part of the test by closing the door of the telephone booth.[45] This simple action "entitled [Katz] to assume that his conversation is not being intercepted."[46]

The second prong is more objective because it takes into consideration the concerns of society as a whole. Professor LaFave believes that the "reasonableness" requirement embedded in the second prong was Justice Harlan's attempt at "giv[ing] content to the word 'justifiably' in the majority's assertion that eavesdropping on Katz was a search because it 'violated the privacy upon which he justifiably relied while using the telephone booth.'"[47] How do we determine what is justifiable? Reasonableness is not enough—"it must be based on something in addition to a high probability of freedom from intrusion."[48] Justice Harlan would have us conduct a balancing test weighing the individual's "sense of security" and

38. *Id.* at 351 (internal citations omitted).
39. LaFave, *supra* note 10, § 2.1(b).
40. *Katz*, 389 U.S. at 361.
41. LaFave, *supra* note 10, § 2.1(b).
42. *Id.* § 2.1(c).
43. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1973-1974).
44. LaFave, *supra* note 10, § 2.1(c).
45. *Katz*, 389 U.S. at 361.
46. *Id.*
47. LaFave, *supra* note 10, § 2.1(d).
48. *Id.* (quoting *From Private Places to Personal Privacy: A Post Katz Study of Fourth Amendment Protection*, 43. N.Y.U. L. REV. 968, 983 (1968)).

the necessity of the conduct as a means of efficient law enforcement.[49] Yet again, we are asked to take a step back and view this from a societal perspective. To what extent is society prepared to give up its rights to privacy to facilitate efficient investigation of a crime?

The *Katz* test's expansive view of Fourth Amendment protection has been applied in many circumstances since its inception. For example, in *Minnesota v. Olson*, it was determined that a defendant had a reasonable expectation of privacy in a home which was not his, but in which he was staying overnight.[50] The Supreme Court took the very practical view that, "[an overnight guest] seeks shelter in another's home precisely because it provides him with privacy, a place where he and his possessions will not be disturbed by anyone but his host and those his host allows inside."[51] In further support of a reasonable expectation, the Court acknowledged that "[w]e are at our most vulnerable when we are asleep because we cannot monitor our own safety or the security of our belongings."[52] The Court was unconcerned with the fact that the defendant had no legal interest in the actual dwelling.[53]

Other Supreme Court justices have come to similar conclusions. In *Rakas v. Illinois*, the Court held "that a person can have a legally sufficient interest in a place other than his own home so that the Fourth Amendment protects him from unreasonable governmental intrusion into that place."[54] Cases like this show just how expansive the applications of *Katz* have been, and how ready courts are to find a privacy interest.

Regardless of the practical implementations of the *Katz* test, its general effect is viewed as one of expanding Fourth Amendment protection.[55] No longer must there be a physical intrusion by police officers in order for someone's Fourth Amendment rights to be violated.

B. United States. v. Jones

Katz asked the question: Is a physical intrusion required for there to be a search? The answer was a resounding "no." *United States v. Jones* came along over forty years later and asked: Is physical intrusion sufficient?[56]

In *Jones,* Antoine Jones was suspected of dealing drugs, and government agents undertook various means of surveilling him.[57] Among those methods was the installation of a GPS tracking device on the underside of Jones' Jeep while it was parked in a public area.[58] The device relayed

49. *Id.* (quoting United States v. White, 401 U.S. 745 (1971)).
50. Minnesota v. Olson, 495 U.S. 91, 96-97 (1990).
51. *Id.* at 99.
52. *Id.*
53. *Id.*
54. Rakas v. Illinois, 439 U.S. 128, 142 (1978).
55. Amsterdam, *supra* note 43, at 385.
56. *See Jones*, 565 U.S. at 400.
57. *Id.* at 402.
58. *Id.* at 403.

information about Jones' movement to officers, who compiled this information with other evidence in formulating charges against Jones of conspiracy to distribute and possession with intent to distribute cocaine.[59] At the trial court level, the judge excluded evidence obtained from the GPS unit while it was parked at Jones' home, but admitted evidence obtained while Jones was travelling in public places.[60] The judge relied on the *Katz* holding by finding, "'[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'"[61]

After a reversal of the conviction by the Court of Appeals, the Supreme Court upheld the reversal on the grounds that the attachment of the GPS device to Jones' car constituted a search, and was therefore a violation of Jones' Fourth Amendment rights.[62] Justice Scalia expressed his understanding of the facts in the most simplified way possible: "The Government physically occupied private property for the purpose of obtaining information."[63] Leaning on the origin of the Bill of Rights, he went on to say, "[w]e have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[64]

Using a textualist approach, Justice Scalia emphasized that the Fourth Amendment has always been closely connected to property and the pre-*Katz* search standards which revolved around trespass theory.[65] While not overruling *Katz*, he pointed out that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[66] He then clearly delineated, "we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."[67] In a world in which so much of our lives involve the "transmission of electronic signals," it is not hard to imagine that many situations will involve both the *Jones* and the *Katz* analysis.

In order to qualify as a non-search, a government action must be able to pass both the *Katz* and *Jones* tests. Either test alone is sufficient to implicate an action as a search. These tests are fairly intuitive when applied to traditional concepts and physical items. But how have these tests (primarily *Katz*) adapted throughout the years of increased technological complexity and the vast, intangible, digital world that now comprises the majority of people's lives?

---

59. *Id.*
60. *Id.*
61. *Id.* (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).
62. *Id.* at 404.
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.* at 409 (emphasis in original).
67. *Id.* at 411.

III. FOURTH AMENDMENT AND CELL PHONES (GENERALLY)

This section will explore how courts have chosen to approach the application of tests, at least in regard to *Katz*, which were developed in an age with very little digital consideration, to the highly digital world in which we live today. The Supreme Court's decision in *Riley v. California* exemplifies the current judicial attitude towards digital items which, in the days of *Katz*, had physical counterparts.[68]

The *Katz* test has been constantly reexamined as new technologies provide complex considerations regarding privacy rights of individuals. Prior to the advent of smartphone technology, there was only so much private information that a person could carry around with them. Chief Justice Roberts has noted, "[m]ost 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—nor would they have any reason to attempt to do so."[69] However, modern cell phones, or "minicomputers," as Justice Roberts aptly refers to them, are fully capable of doing just that.[70] In *Riley*, the Supreme Court demonstrated the judiciary's heightened scrutiny of searches involving smartphones and similar electronic devices.[71]

Riley itself is a combination of two appeals, the first brought by David Riley appealing a warrantless search of his smartphone "looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with guns."[72] The search produced evidence which linked Riley to a car used in a previous shooting incident.[73] The second case involved an appeal by Brima Wurie of police use of a "flip phone," again without a warrant, to locate his apartment, wherein they found "crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash."[74]

The Court began its analysis by distinguishing cases which had laid the previous groundwork for when a warrant was required for a search incident to an arrest. *Chimel v. California* established two central interests that weigh in favor of circumventing the warrant requirement: officer safety and the preservation of evidence.[75] The *Chimel* analysis was applied in *United States v. Robinson* where Robinson was being pat down when an

68. *Riley*, 134 S. Ct. at 2473.
69. *Id.* at 2489.
70. *Id.*
71. *Id.* at 2473.
72. *Id.* at 2480-81.
73. *Id.* at 2481.
74. *Id.*
75. *Id.* at 2483 (citing Chimel v. California, 395 U.S. 752 (1969) (holding that it is reasonable for an officer "to search the person arrested in order to remove any weapons that the latter might seek to use," and "search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction")).

officer felt something in his coat pocket.[76] The item turned out to be a "crumpled cigarette package," and the officer proceeded to open it, finding capsules of heroin.[77] The *Robinson* Court held this search unreasonable because it did not implicate either of the *Chimel* factors—"Robinson was unlikely to have evidence of the crime of arrest on his person," and "it could not be justified as part of a protective search for weapons."[78]

But the Court refused to apply the *Robinson* and *Chimel* reasoning to searches regarding cell phones.[79] Cell phones are a different animal. Searches of cell phones do not present comparable risks as those searches considered by *Robinson* and *Chimel*—"a search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*."[80]

In the *Riley* decision, Justice Roberts paints the picture of a person carting around a trunk filled with all of the personal items they had collected over the past several years.[81] Cell phones represent not just the ability to carry around this extreme volume of information, but because of the "many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," cell phones could essentially allow for "[t]he sum of an individual's private life to be reconstructed."[82]

There are other aspects of a cell phone search which troubled the Court. Particularly, the Court was disturbed by the pervasiveness present in a cell phone search as opposed to a physical search. Whereas, in the past, a "police officer searching an arrestee might have occasionally stumbled across a highly personal item such as a diary," in today's society, "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[83] In particular, the information exposed could include a "wealth of detail about her familial, political, professional, religious, and sexual associations."[84]

Clearly, the Court was greatly concerned about both the quantity and quality of the information which could be exposed by a cell phone search. The concern for this type of information is not new, as Justice Roberts noted the Learned Hand quote from 1926, "that it is 'a totally different thing to search a man's pockets and use against him what they contain, from

76. *Id.* at 2483 (citing United States v. Robinson, 414, U.S. 218 (1973)).
77. *Id.*
78. *Id.*
79. *Id.* at 2485.
80. *Id.*
81. *Id.* at 2489.
82. *Id.*
83. *Id.* at 2490.
84. *Id*. (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

ransacking his house for everything which may incriminate him.'"[85] Smart phones and their progeny have simply made this information much more accessible to anyone who possesses them. *Riley* made clear that the accessibility of that information does not make it any less sacrosanct—"[t]he 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."[86]

Courts will clearly look beyond the label of "phone." Smartphones will be treated similarly to computers or any other storage device capable of containing the intimate details of an individual's life. How does this bear on the issue of Emergency functionality? To address that particular question, we must turn to more nuanced case law. Simply possessing someone's phone is not the same as diving through the minutia of their calendar, email, and web browsing history. Just as the Court in *Riley* was concerned about the quantity and quality of information potentially exposed by a search, there must surely exist a spectrum of discoverable information. At some point along this spectrum the quantity of the information exposed is so great, or the quality of the information exposed so private, that courts will find a search has taken place.

IV. THE MAGSTRIPE CASES

Where, on the spectrum, does the information at stake in our hypothetical case lie? What is the quality and quantity of information exposed when an officer utilizes Emergency? As will be discussed later in this section, though Professor Kerr[87] and I disagree as to the holdings of the cases, we agree that the facts of the Emergency case align closely with the fact patterns of a group of cases currently being litigated through the circuit courts—the Magstripe Cases.

The question at issue is whether there is a reasonable expectation of privacy in the magnetic stripe (magstripe) of a credit card. Typically, the information contained in the magstripe is reflective of what is printed on the front of the card, i.e. name, account number, and expiration date.[88] However, that information is capable of being reprogrammed to contain anything—subject to a limit of 79 letters and 147 numbers.[89] This is particularly useful to criminals who purchase stolen credit card data, but are not in possession

85. *Id.* at 2490-91 (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2nd Cir. 1926)).

86. *Id.* at 2495.

87. Orin Kerr is a professor at George Washington University Law School, and is a scholar of criminal procedure and computer crime law.

88. Orin Kerr, *Is Credit Card Skimming a Fourth Amendment Search?,* WASHINGTON POST (July 29, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/29/is-credit-card-skimming-a-fourth-amendment-search/?tid=a_inl&utm_term=.d4cd92ee9c05.

89. *Id.*

of the actual cards.[90] As Professor Kerr points out, "the buyer can take an old credit card and re-encode the old card with information from the stolen credit card number. The buyer can then use the old credit card as if it were the stolen card."[91]

Law enforcement, upon lawfully retrieving what they believe to be stolen credit cards, can skim the information from the magstripe to see if it matches the information on the front of the card.[92] If it does not match, they are alerted to some kind of fraud.[93] But, is the skimming of the credit card information a Fourth Amendment search? The Fifth, Sixth, and Eighth Circuits have all weighed in on the issue and, though the three have come to similar conclusions, there is some speculation that a circuit split is in the making.[94]

A. United States v. Bah

The Sixth Circuit was the first to address this issue in *United States v. Bah*.[95] Mamadou Bah and Allan Harvey were stopped by a police officer for speeding in a construction zone.[96] A lawful search of their vehicle and their persons turned up eighty-six cards; including credit, debit, and gift cards.[97] The officer, "without a warrant—then used a magnetic card reader, or "skimmer," to read the information encoded on the magnetic strips of [some of the cards]."[98] As expected, "a 'majority, if not all' of the magstripes had been re-encoded so that the financial information they contained did not match the information printed on the front and backs of the cards."[99] Subsequent investigation showed that several of the accounts linked to the cards "had already incurred fraudulent charges."[100]

The trial court ruled that the evidence from the magstripes should not be excluded because "'[a]n owner or possessor of a credit, debit, or gift card has no reasonable expectation of privacy in the data encoded on the magnetic strip.'"[101] The circuit court upheld the lower court's holding regarding the magstripes, and it expounded with its own reasoning.[102] Broadly, the circuit court held that "[n]o 'search' occurred when law enforcement read the

90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. Orin Kerr (@OrinKerr), TWITTER (Oct. 14, 2016, 1:15 PM), https://twitter.com/OrinKerr/status/787024088304721920.
95. 794 F.3d 617 (2015).
96. *Id.* at 621.
97. *Id.* at 622-23.
98. *Id.* at 623.
99. *Id.*
100. *Id.* at 624.
101. *Id.* at 625 (quoting magistrate's decision, *U.S. v. Bah*, No. 2:13-CR-48, 2013 WL 5652647, at *7 (E.D. Tenn. Aug. 8, 2013)).
102. *Id.* at 630.

magnetic strips on the backs of the fraudulent cards because: (1) the scans did not involve a physical intrusion of a constitutionally protected area—as required under the trespass-based search analysis; and (2) the scans did not violate the cardholders' reasonable expectation of privacy."[103]

Regarding the physical intrusion aspect, the court examined the decisions of *Jones* and *Florida v. Jardines*, both of which involved the government "physically intruding into an area."[104] This situation was distinct from those because "'[s]liding a card through a scanner to read virtual data . . . does not involve' any such physical invasions."[105]

In applying the *Katz* test, the court disregarded the argument of whether the men had a subjective expectation of privacy in the magstripes.[106] That issue was irrelevant because, as the court determined, "neither Bah nor Harvey [held] a reasonable expectation of privacy in the magnetic strips. . . . Such an expectation of privacy is not one that society is prepared to consider is reasonable."[107] The court was unwilling to recognize a reasonable privacy interest in the magnetic strips because they are "routinely read by private parties at gas stations, restaurants, and grocery stores to accelerate financial transactions."[108] The information on the strips, specifically the account number, "is routinely shared with cashiers every time the card is used."[109] The court noted that "'society is not prepared to accept as legitimate an asserted privacy interest in information that any member of the public may see.'"[110]

Moreover, the court was not persuaded by the amount and kind of information that would potentially be exposed by such an action.[111] It distinguished the Supreme Court's ruling in *Riley*, regarding searches of cell phones, computers, and cassettes, on the basis that concerns regarding the quantity and quality of information exposed by those searches were not at issue here.[112] Specifically, the court said "[t]he storage capacity of the magnetic strip of credit, debit, or gift card pales in comparison to that of a computer hard drive, cell phone, or even audiocassette," "a reading of it . . . would not allow officers to reconstruct an individual's private life," and "[it] is not the highly personal information an individual would expect to keep private."[113] Furthermore, the information in the credit card "is intended to be read by third parties," and "literally has no purpose other than to be provided

---

103. *Id.*
104. *Id.* (citing *Jones*, 565 U.S. 400 (2012); Florida v. Jardines 133 S. Ct. 1409 (2013)).
105. *Id.* (quoting United States v. Alabi, 943 F. Supp. 2d 1201 (D.N.M. 2013)).
106. *Id.* at 630.
107. *Id.* at 630-631.
108. *Id.* at 631.
109. *Id.*
110. *Id.* (quoting United States v. DE L'Isle, No. 4:14-CR-3089, 2014 WL 5431349, at * 7 (D. Neb. Oct. 24, 2014)).
111. *Id.* at 632.
112. *Id.* at 633.
113. *Id.*

to others to facilitate financial transactions."[114] It was important to the court that the extent of the information to be exposed was known, and they withheld judgment regarding situations where either the contents of the device were truly unknown or where future storage capacity allowed for a much greater amount of private information to be stored on these kinds of cards.[115]

B. United States v. DE L'Isle

The case of *United States v. DE L'Isle* has many similarities to *Bah*.[116] Just as in *Bah*, Eric-Arnaud Benjamin Briere DE L'Isle was pulled over for a routine traffic stop—following too closely to a semi-tractor trailer.[117] The police officer smelled marijuana and lawfully obtained fifty-nine credit, debit, and gift cards during his subsequent search of the vehicle.[118] "DE L'Isle was charged with possession of fifteen or more counterfeit and unauthorized access devices," and he moved to suppress the evidence gained from the skimming of the cards.[119] DE L'Isle argued that the account information contained in the strip was the "type of information that the Supreme Court would consider a legitimate privacy interest."[120]

The discussion by the court was also similar to *Bah*; there was no physical intrusion into the card to offend the *Jones* test.[121] In this case, however, the court addressed the issue of whether the defendant could have had a subjective expectation of privacy in the cards. The answer was 'no' because, "the purpose of a credit, debit, or gift card is to enable the holder of the card to make purchases, and to accomplish this, the holder must transfer information from the card to the seller, which negates an expressed privacy interest."[122] Similarly to *Bah*, this Court found that DE L'Isle had no expectation of privacy in the cards that society was prepared to accept as reasonable.[123]

What sets *DE L'Isle* apart from *Bah* is the argument presented by the dissenting Judge Kelly in *DE L'Isle*.[124] The dissent sought to remand the case in order to gather more information, but also took a starkly different approach to the expectation of privacy issues from the majority.[125]

---

114. *Id.* (quoting *DE L'Isle*, No. 4:14-CR-3089, 2014 WL 5431349 (D. Neb. Oct. 24, 2014)).
115. *Id.* at 633.
116. *DE L'Isle*, 825 F.3d 426 (8th Cir. 2016).
117. *Id.* at 429.
118. *Id.*
119. *Id.*
120. *Id.* at 431.
121. *Id.*
122. *Id.* at 432.
123. *Id.*
124. *Id.* at 433.
125. *Id.* at 434.

Judge Kelly's main concern was the ease with which one could re-write the information contained on a magstripe.[126] She invoked the "straightforward principle that law enforcement conducts a Fourth Amendment 'search' when it reads the contents of rewritable digital storage media."[127] Under Judge Kelly's theory, to the extent that the magstripes are easily rewritable, they should be treated more like digital storage devices or mini-hard drives.[128] "If a magnetic stripe card is a digital storage device, albeit one whose storage capacity is limited, . . . reading the data on it is a Fourth Amendment search."[129] She goes on to give examples of legal applications of the rewritable functionality; a cardholder could "rewrite the data on the magnetic stripe of a card she had no more use for to 'MYBANKACCOUNTPASSWORDIS78911Y783,' so that she could recover her password in the event she forgot it."[130]

Her point is that police officers cannot know for sure what they are going to find when they skim the magstripe. It might be illegal, but it might not be. It could in fact be the kind of personal information that the Fourth Amendment was intended to protect. She goes further to say that, "individuals have a reasonable expectation of privacy even in so-called single-purpose containers, 'those rare containers' whose 'distinctive configuration . . . proclaims [their] content.'"[131] Examples include things like "cereal boxes, guitar bags, gun cases, and the like."[132] In other words, it doesn't matter if officers know what they are going to find in the container—i.e., cereal—and that the possible exposure of information is limited. "The Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view."[133]

Judge Kelly is not the only opponent of the judicial trend which proclaims no expectation of privacy in magstripes. Professor Orin Kerr has been very vocal in his belief that a reasonable expectation of privacy exists in the information encoded on a magstripe.[134] In his opinion, swiping the magstripe "is a classic kind of Fourth Amendment search, retrieving information stored inside a storage device."[135] He sees it as irrelevant that the information typically matches what is on the outside of the card.[136] Instead, he emphasizes one of the same points made by Judge Kelly—ultimately, police officers do not know what information they are going to find when

126. *Id.*
127. *Id.* (citing United States v. James, 353 F.3d 606, 613 (8th Cir. 2003)).
128. *Id.*
129. *Id.*
130. *Id.* at 435.
131. *Id.* at 436.
132. *Id.*
133. *Id.* at 435 (quoting United States v. Ross, 456 U.S. 798, 822-23 (1982)).
134. Kerr, *supra* note 88.
135. *Id.*
136. *Id.*

they swipe the card.[137] Judge Kelly was particularly troubled by this point, as she said, "the results of a search cannot be used to justify its legality."[138] She continued, "[w]e have had frequent occasion to point out that a search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from its success."[139] As an example, she supplied that whether full of contraband or legitimate papers, once an officer opens a briefcase, a search has been conducted.[140]

Professor Kerr continues on to examine the argument made by the majority in *DE L'Isle*, that there is no expectation of privacy because the card number is handed out every time the card is used.[141] In his opinion, the situation is no different than if he is "working on a blog post from [his] laptop at home," and the police want to hack into his laptop based solely on the fact that he "plan[s] to publish the post eventually."[142] In other words, whether information has been given out in the past, or would be given out in the future, does not defeat Fourth Amendment protection of that information at the present moment.[143]

Following the Fifth Circuit's holding that there is no reasonable expectation of privacy in a magstripe, Professor Kerr again sought to clarify two points of his argument.[144] First, he argues that the decisions resting on the amount of information exposed are mistaken in their reasoning.[145] He cites *Arizona v. Hicks* to show that the amount of information potentially exposed by the act should not be determinative. In *Hicks*, "[t]he officer's act was not likely to reveal a lot of information, and the only information was the manufacturer's information about the serial number."[146] Even here, where the exposure of information would be minimal, "the Court ruled that moving the turntable was a search."[147] Professor Kerr also uses this example to refute the argument regarding quality or type of information.[148] In *Hicks*, the information at stake was a serial number—"just meaningless numbers assigned by a company that most users don't know about and would never care to see."[149] In this respect, the information in *Hicks* contained even less

137. *Id.*
138. *DE L'Isle*, 825 F.3d at 435.
139. *Id.*
140. *Id.*
141. *See id.* at 432.
142. Kerr, *supra* note 88.
143. *Id.*
144. Orin Kerr, *Fifth Circuit Rules on Whether Scanning the Magnetic Stripe on a Card is a Search*, WASHINGTON POST (Oct. 16, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/16/fifth-circuit-rules-on-whether-scanning-magnetic-stripe-on-a-card-is-a-search/?utm_term=.53088802447c.
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*

personal information than that which is at stake in the magstripe cases.[150] His conclusion is that "like moving the turntable in *Hicks*, . . . scanning the magnetic stripe on the back of a card 'expose[s] to view concealed portions of the [item] or its contents' and is therefore a search."[151]

Professor Kerr's second argument is that courts have misplaced their focus in these cases.[152] In his opinion, rather than concerning themselves with the nature of the information obtained, they should be looking at the method used to obtain it—"forcibly exposing information from inside a person's Fourth Amendment effects, which is as core of a search as you can get."[153] His opinion is that the courts should be sticking to a bright-line rule in these situations—one that disregards how minimal the information accessed might be.[154]

Whether on the side of the majority opinions in these cases, or on the side with Judge Kelly and Professor Kerr, it is clear that although there is not yet a circuit split, intelligent minds disagree regarding the privacy implications of these facts. Because of the factual similarities between the magstripe cases and the Emergency hypothetical case, whichever view is adopted in the magstripe cases will be highly indicative of how the Emergency case is decided.

V. ANALYSIS AND APPLICATION

As of the writing of this Note, only one case has directly addressed the issue in question here. In *State v. Hill*, a Georgia police officer used a phone left in the back seat of a taxi cab to place a call out to 911.[155] By doing so, he obtained the identifying information of the phone owner, Hill, who was subsequently charged with theft of services for fleeing the cab without paying his fare.[156] This was done through the Emergency feature, and the passcode protected information on the phone was not accessed.[157] Though the reasoning of that court differs from what has been set forth here, the conclusion is the same—the information obtained was not entitled to protection under the Fourth Amendment. The arguments made by that court are incorporated into this section.

In line with the majority decision from *DE L'Isle* and the holding in *Bah*, courts should find that there is no reasonable expectation of privacy in a phone number, such that a police officer's use of the Emergency functionality of the phone to retrieve the number should not be considered a Fourth Amendment search for three reasons: (1) the quality and quantity of

150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. 338 Ga. App. 57 (Ga. Ct. App. 2016).
156. *Id.*
157. *Id.*

the information exposed does not trigger Fourth Amendment protection, (2) it qualifies as a non-search under both the *Jones* test and (3) the *Katz* test. Moreover, even if a court were to find this action to be a search, it is possible that the warrant requirement would be waived through an application of the balancing test (weighing "the degree to which it intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests")[158] or if it fell into one of the major exceptions to the warrant requirement.

First, the quality and quantity of information accessed in this case do not rise to the level of being protected by the Fourth Amendment search requirements. It is important, before beginning the analysis, that consideration be given not only to the nature of the information being exposed, but also the manner in which it is being accessed. As stated previously, the Emergency functionality of the phone is accessible from the phone's lock screen—without needing to enter or break the phone's passcode. This is important because the data stored on the phone is not exposed to the person utilizing Emergency. The Emergency screen itself is a number pad from which any telephone number can be dialed—it is not restricted to dialing 911. None of the phone's contacts are displayed. Under the proposed scenario, the only information accessible by a police officer is the telephone number associated with the cell phone. This would be achieved by dialing 911—the telephone number of the phone would display to the 911 operator—and then the officer would communicate with the call center operator to get the number of the phone.

It should be distinguished that the identity of the phone owner is not exposed throughout this process, only the telephone number associated with the phone. Should they choose to do so, police officers would be able, through the warrant process, to access the owner's identity from the telephone service provider.

But even if the owner's identity was among the information to be exposed, the court in *State v. Hill* did not consider identifying information—including things like phone number, name, and birthdate—to be among the types of information protected by the Fourth Amendment.[159] Particularly, the court held "that [the defendant] had no legitimate expectation of privacy in this information."[160] The court went on to cite over a dozen cases from various jurisdictions indicating that this kind of information was not the kind "about which a person can have a reasonable expectation of privacy."[161] This categorical distinction of a class of identifying information which is not entitled to Fourth Amendment protection is in line with the *Katz* "reasonable expectation of privacy" test. However, this categorical exclusion is distinct from *Katz* analysis because it was not included in the original *Katz* case, and

158. Totten, *supra* note 12, at 2484.
159. *Hill*, 338 Ga. App. at 58.
160. *Id.*
161. *Id.* at 59.

has developed over time through various court decisions. Moreover, the court refused to extend *Riley* reasoning to the identifying information "simply because that information was associated with a cellular phone account rather than a landline phone account or a piece of physical mail."[162]

The Georgia Court of Appeals in *Hill* made a further distinction regarding the protections provided by the Fourth Amendment. Namely, the Court noted that, "although the content of personal communications is private, the information necessary to get those communications from point A to point B is not."[163] This is a significant point, and it stands in stark contrast to the view taken by Professor Kerr. The Georgia court focused very heavily on the quality of information that is being accessed, whereas Professor Kerr, and those who believe similarly, are concerned more about the method through which the information is obtained—"[c]alling 911 pushes out the number from the phone, and [Kerr thinks] that forced revealing of the number should count as a search of the phone."[164]

The *Hill* majority's counterpoint to Kerr is that it simply does not matter that a police officer, rather than a private citizen, was the one doing the 'forcing.'[165] The court stated explicitly that this distinction "does not change our conclusion that the information was not subject to Fourth Amendment protection."[166] It went on to cite case law permitting government actors to take actions ranging from causing a cell phone to emit location information to removing the phone's battery in order to obtain the serial number associated with the phone.[167] In each of these cases, the reviewing court held that no search had taken place.[168]

As an aside, also available in the Emergency screen is a Medical ID function. The Medical ID screen may include name and birthdate of the phone's owner, emergency contacts, and medical allergy information, similar to a medical ID bracelet or necklace. The Fourth Amendment implications of this functionality lies beyond the scope of this Note, but it will suffice to say that the information included in the Medical ID section is loaded voluntarily by the owner for the sole purpose of being utilized by a third party for that owner's benefit.

How does the access to telephone number information square with the different Fourth Amendment search tests? Under the *Jones* analysis, assuming that the police are in lawful possession of the phone, accessing the Emergency function likely does not offend common-law trespass theory.

---

162. *Id.* at 61.

163. *Id.* at 59.

164. Orin Kerr, *Calling 911 From A Phone To Obtain Its Number Does Not 'Search' It, Court Rules*, WASHINGTON POST (July 15, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/15/calling-911-from-a-phone-to-obtain-its-number-does-not-search-it-court-rules/?tid=a_inl&utm_term=.c1626cce67cc.

165. *Hill*, 338 Ga. App. at 60.

166. *Id.*

167. *Id.* at 60-61.

168. *Id.*

Looking strictly at the physical nature of the action, officers using their fingers to swipe and touch a glass screen does not rise to the same level of attaching a GPS monitoring device to someone's car, as was the case in *Jones*.[169] It would be much more akin to, though still not the same as, the officer's actions in *Hicks*, where the officer moved stereo equipment in order to retrieve serial numbers of what he suspected to be stolen goods.[170] The immediate hypothetical is distinguishable even from *Hicks*, in that *Hicks* still involved a physical moving of items and uncovering of information which the court determined was,

> [A] "search" separate and apart from the search for the shooter, victims, and weapons that was the lawful objective of his entry into the apartment. Merely inspecting those parts of the turntable that came into view during the latter search would not have constituted an independent search, because it would have produced no additional invasion of respondent's privacy interest.[171]

The violation committed by the officer in *Hicks* sounds in physical trespass. His lawful search gave him access to the apartment, but it did not give him the right to conduct "a 'search' separate and apart" from the lawful one.[172] *Hicks*, while pre-dating *Jones*, and not a part of the *Jones* analysis, serves to show the high level of sensitivity with which trespass theory is applied to Fourth Amendment jurisprudence.

Clearly, the physical trespass reasoning is insufficient when dealing with modern technology. Many invasive searches can take place in today's world without the government physically intruding upon anything. So, how does this action hold up under *Katz* analysis?

First, is there a subjective expectation of privacy in the information accessed by Emergency? For the *Katz* court, it was enough to satisfy this test simply that Katz had shut the door to the telephone booth.[173] That which he wanted to keep private was the sound of his words. Though he may have been plainly visible in the booth to anyone passing by, the action of closing the phone booth door indicated that he had a subjective expectation of privacy in the things that he said. This portion of the test is difficult to apply outside of a specific case, because the facts and people involved will most likely change the analysis, but it is fair to analogize the phone booth door to the iPhone lock screen. By creating a passcode and engaging the lock screen function, the user of a phone has asserted that the information behind that screen is private. By this analogy, anything in the phone which must be accessed by

169. *Jones*, 565 U.S. at 403.
170. *Hicks*, 480 U.S. at 323.
171. *Id.* at 324-325.
172. *Id.* at 324.
173. *Katz*, 389 U.S. at 361.

inputting the passcode is entitled to a subjective expectation of privacy. But the instant case involves information and functionality which exists outside of that passcode barrier, and by that logic would not automatically be presumed to have a subjective expectation of privacy.

Moreover, a user's awareness of the Emergency function decreases that person's subjective expectation of privacy. As it has been pointed out that the Government could "diminish each person's expectation of privacy" by letting us all know that we are subject to constant surveillance, to the extent that an iPhone user is aware that his or her phone can be used to place an Emergency call without unlocking the passcode, he or she has lost the subjective expectation that it would not be used in this way. For these reasons, the Emergency function of the phone sits "outside the phone booth" and should not be afforded a subjective expectation of privacy.

One critique of this position is that the Emergency functionality on the phone is not set up voluntarily by the phone's owner. It is built into the operations of the phone. Yes, the case against a subjective expectation would be made much stronger if there were an opt-in or opt-out setting which each user could utilize or ignore at his or her preference. However, though the situation is not ideal, it is still fair to preclude smartphone users from asserting a subjective expectation of privacy in the phone's Emergency functionality.

Even if a particular user could establish a subjective expectation of privacy, *Katz* requires that it must be an expectation which "society is prepared to recognize as 'reasonable.'"[174] It is here where all of the modern computer, smartphone, and magstripe cases come into play. As *Riley* makes clear, our society is prepared to recognize an expansive privacy interest in smartphones for the simple reason that they are much more appropriately considered computers—which also happen to make phone calls.[175] The information contained in smartphones touches nearly every aspect of a person's life and, from the criminal's perspective, can implicate someone of wrongdoing much faster and easier than a search of the most hidden spaces of his house.

The critical point here is that this vast world of information contained in a smartphone is not compromised by the use of the Emergency function. It is unquestioned that an officer would need a warrant in order to penetrate to the actual substance of the device wherein all of the applications, emails, calendars, and messages are contained that implicate the deep privacy interest.[176] But that is not happening here. The only information to be exposed by this search is a ten-digit number associated with the device. Justice Roberts' vision of a person carting around a trunk full of all of their personal items is inapplicable to this limited use of the phone.

---

174. *Id.* at 352.
175. *See Riley*, 134 S. Ct. 2473.
176. *See Id.*

Furthermore, *Riley*'s broad recognition of privacy is not without limits. The *Katz* decision itself conceded that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[177] The magstripe cases keyed in on this reasoning in noting that a person has no privacy interest in the number programmed into the card because, "the purpose of [a card] is to enable the holder of the card to make purchases, and to accomplish this, the holder must transfer information form the card to the seller, which negates an expressed privacy interest."[178]

The court in *Hill* incorporated this reasoning into its decision, and it expounded, saying "[t]his rule applies even where the person revealing information intended its use by the third party to be limited."[179] The reasoning, according to the court is that, "[b]y using a phone, a person exposes identifying information to third parties, such as telephone companies, and assumes the risk that the telephone company may reveal that information to the government."[180] On this very narrow point, I disagree with the *Hill* majority. While I agree with the Court's ultimate conclusion, its application of an assumption of the risk principle goes too far, and has far reaching privacy implications that the Court probably did not intend. The mere consumption of a product or service should not then entitle the providing company to disclose information about that consumption to the government. So, while the assumption of the risk argument can contribute to the analysis, it should not be alone sufficient to warrant government intrusion into an individual's private information.

The practical use of a telephone number bears great similarity to the number encoded on a credit card stripe. The purpose of a telephone number is to serve as a locator, allowing others to actively contact a phone's user. Anytime a user places a call, his or her number is automatically given out to whoever the user is trying to contact—assuming the user is not utilizing an identity-blocking service. In fact, it is exactly that kind of information which someone "knowingly exposes to the public" every time they use their phone.[181]

The force of the argument presented by Judge Kelly's dissent in *DE L'Isle* is lessened when applied to telephone numbers, because the number associated with the phone is not manipulable in the same way that the number encoded in a credit card magstripe is manipulable. Judge Kelly was concerned by the similarities between the magstripe and a regular container, in which someone, through the process of re-encoding, could be storing their

177. *Katz*, 389 U.S. at 351.

178. *DE L'Isle*, 825 F.3d at 432.

179. *Hill*, 338 Ga. App. at 60 (citing United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016)).

180. *Hill*, 338 Ga. App. at 60.

181. *See Katz*, 389 U.S. at 351.

password for an account or an admission of guilt to some crime.[182] The information gathered by police officers when they use the Emergency function is nothing more than the ten-digit number associated with the phone.

Finally, even if a court were to find that a search had taken place, it is possible that the warrant requirement would be waived. There are two main ways in which this can happen: (1) through an application of a balancing test which essentially weighs the individual's privacy interest with legitimate governmental interests, or (2) if the facts of the case happen to fall within one of the recognized exceptions to the warrant requirement. Regarding the first option, legitimate governmental interests commonly boil down to just two considerations—officer safety and the destruction of evidence.[183]

Both of these possibilities involve heavily fact-based inquiries, and the benefit of trying to apply them here is minimal. However, there are some general observations that can be made regarding the interests of the balancing test. As argued above, it can be said that the individual privacy interest at stake is relatively small. As the court in *Hill* pointed out, many courts have held that general identifying information is not the kind in which an individual has a reasonable expectation of privacy.[184] It can also be said that the governmental interest is small, because it would be a rare circumstance for this narrow use of Emergency to implicate officer safety or an avoidance of the destruction of evidence.

There is certainly not a clear-cut answer as to whether or not use of the Emergency function to retrieve a phone number would qualify as a search, but I believe that after consideration of the qualitative and quantitative factors of the information exposed, and an application of the *Katz* and *Jones* tests, this kind of action is not a search, and therefore no warrant should be required for police officers to make use of this tactic. Furthermore, it is possible that the warrant requirement would be waived even if this action was found to be a search.

CONCLUSION

The touchstone of Fourth Amendment applications begins and ends with reasonableness. True, there are certain bright-line rules giving definition to the concept of a search. But, barring a violation of those rules, judges must take into consideration all of the factors involved and make a decision which properly balances both the interests of individual privacy and the efficiency of police investigation.

It is an oversimplification of the issue, and ignores the need for expedient investigation, to simply say police should be required to get a warrant in situations where the Emergency function is used. It is equally

182. *See DE L'Isle*, 825 F.3d at 435.
183. Totten, *supra* note 12, at 2484.
184. *Hill*, 338 Ga. App. at 58.

dangerous to expand police power to conduct unwarranted activities which exist at the fringes of Fourth Amendment protection without justification.

In this case, however, there is ample justification to allow police to utilize the Emergency feature of a smartphone without first obtaining a warrant in order to ascertain the identity of its owner. The quantity of information exposed is small; the information is limited to the ten digits which make up the associated telephone number. The number is not easily manipulable such that this portion of the device could be considered a container—no passwords or messages written by the phone's owner will be discovered by the police officer's call. Moreover, the quality of the information is not the kind to which courts have applied Fourth Amendment protection. As the Georgia court acknowledged in *State v. Hill*, basic identifying information such as name, age, and phone number is not the kind to which individuals are entitled a privacy interest.

Additionally, the way in which the information is retrieved does not trigger Fourth Amendment protection. Previous cases have shown great concern for intrusions upon the data contained within a phone (typically protected by the phone's passcode). In this case, the information gathered is all outside of the passcode's protection, and does not invoke *Riley* protection because the "trunk" full of calendars, emails, communications, and internet history is not exposed to the officer in any way.

Fourth Amendment protection is not implicated by an application of the *Jones* test. There is no physical intrusion into the phone, rather, contact with the phone is purely external in this situation.

Nor is protection required under an application of the *Katz* test. A subjective expectation, though it may be able to be shown case to case, is difficult to prove, and ultimately less determinative of the issue than the objective requirement. From an objective standpoint, there are sufficient reasons to hold that an expectation of privacy in this information is not something which society is prepared to accept as reasonable. Among those are the *Hill* majority's analysis of the kind of information at issue, and the fact that a telephone number is knowingly disclosed to third parties as a normal function of its use.

For these reasons, police use of the Emergency function on a smartphone should not be considered a search under the Fourth Amendment, and therefore a warrant should not be required before a government actor is able to make use of the function.