ISEARCH INTO THE IPHONE

Kristen Vogl[*]

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
>
> *Fourth Amendment of the U.S. Constitution*

I. SYLLABUS

The Fourth Amendment's application to real life scenarios is ever-changing and developing. When the Fourth Amendment was ratified December 15, 1791, the Founders never could have anticipated the

* Staff Attorney for the Florida Fourth District Court of Appeal. J.D., 2015, University of Florida Levin College of Law; B.A., 2012, University of Florida. I would like to thank Professor Jon Mills for his guidance in writing this Note and Professors E. Lea Johnston and John F. Stinneford for their passion in teaching criminal law. I would also like to thank the editors of the *Journal of Technology Law & Policy* for their hard work and attention to detail.

technology that would become available in the next hundreds of years.[1] The U.S. Supreme Court has been able to view the language of the Fourth Amendment and adopt it to cases as it sees fit despite the advancements in the definitions of houses, papers, and effects.[2] However, this has not come without significant challenges. In this context, the courts have considered whether listening to an electronic recording device attached to a telephone booth,[3] installation and use of a pen register,[4] and use of a thermal-imaging device aimed at a private home[5] are all considered "searches" according to the language of the Fourth Amendment.

The U.S. Supreme Court affirmed that "a few specifically established and well-delineated exceptions" can exist to the warrant requirement in the Fourth Amendment.[6] This has caused more questions and concerns from the courts as they each continue to draw the line as to what constitutes a search and if that search falls under an exception.[7]

Law enforcement officers have often explored suspects' cell phones without first obtaining a valid warrant with probable cause signed by a judge. This has proved to be alarming with 91% of American adults possessing a cell phone and 56% possessing a smartphone as of May 2013.[8] Cell phones have the capacity to contain personal identification, location (Global Positioning System), and any other content accessed by or given to third-parties. This information can be used, as well as abused, by all members of the public. As stated in *Riley v. California*, "[c]ell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals."[9]

This Note aims to provide insight into the history of the "search" and its adaptation to the modern world of cellular telephones. Although the Fourth Amendment has been the pinnacle of cases for cellular telephones, the Fifth Amendment is emerging in importance as access to the cellular phone advances. The criminal justice system's issue throughout history has remained clear: how much privacy are citizens willing to lose in order to stay protected?

---

1. *Amendment IV*, NATIONAL CONSTITUTION CENTER, http://constitutioncenter.org/constitution/the-amendments/amendment-4-search-and-seizure.

2. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967); United States v. White, 401 U.S. 745 (1971); Kyllo v. United States, 533 U.S. 27 (2001).

3. *Katz*, 389 U.S. at 349.

4. Smith v. Maryland, 442 U.S. 735, 736 (1979).

5. *Kyllo*, 533 U.S. at 29.

6. *Katz*, 389 U.S. at 357.

7. *See, e.g.*, Kentucky v. King, 131 S. Ct. 1849 (2011).

8. State v. Earls, 70 A.3d 630, 638 (N.J. 2013).

9. 134 S. Ct. 2473 (2014).

II. HISTORY OF THE FOURTH AMENDMENT

The Fourth Amendment protects people by ensuring security in their houses, papers, and effects against unreasonable searches and seizures. As promising as the Fourth Amendment sounds, the Founders did not write any solidified guidelines on how to correctly enforce that protection. This led to mixed results. Early in the 1900s, the Court had a single question to decide: whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wiretapping, amounted to a violation of the Fourth Amendment.[10] The Court sidestepped answering this issue by stating:

> Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.[11]

As electronic developments continued and advanced, the Court brought forward considerations of broader Fourth Amendment implications.[12] These implications eventually could not be ignored and consequently led to evolving interpretations of the 'Five W's': who was protected; when are people protected; where are people protected; what is a search; and why—what is reasonable.

A. Katz v. United States

In 1967, a man named Charles Katz was in a telephone booth in Los Angeles speaking to his clients on the phone.[13] The topic of their conversations was wagering information that spread to Miami and Boston.[14] Unbeknownst to Mr. Katz, Federal Bureau of Investigation (FBI) agents had attached an electronic listening and recording device to the outside of the telephone booth that Mr. Katz was located in.[15] Mr. Katz was convicted under an eight-count indictment for transmitting this

10. Olmstead v. United States, 277 U.S. 438, 455 (1928).

11. *Id.* at 455-56.

12. The Court did not always choose to decide these implications. *See* Silverman v. United States, 365 U.S. 505, 509 (1961) ("We need not here contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society.").

13. Katz v. United States, 389 U.S. at 348-49.

14. *Id.*

15. *Id.* at 348.

type of information using a "wire communication facility."[16]

The majority made a radical realization for its time: "the Fourth Amendment protects people, not places."[17] The main inquiry was not the location of Mr. Katz in a telephone booth; but rather, what Mr. Katz intended to do in the telephone booth. The majority's rule came down to two simple, but distinct, concepts: (1) "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection; (2) But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[18]

The Court recognized the significance of the public telephone in private conversations, making a huge step from the 1900s.[19] Mr. Katz sought to exclude, not the naked eye, but the "uninvited ear."[20] Because Mr. Katz's privacy was violated when he relied on his words to remain within the context of his conversations, the government's activities constituted a search.[21] It took the Court until this time to acknowledge that people are entitled to know, regardless of where they may be located, that they will remain free from unreasonable searches and seizures.[22]

What is significant about *Katz* is that the majority opinion, although revolutionary for its time, is not what is most commonly cited. The concurrence, written by Justice Harlan, focuses on defining the protection that is afforded to people by the Fourth Amendment.[23] Justice Harlan recognizes a type of circular logic between the Fourth Amendment's protections of people, while generally having to reference a place to understand what protection can be afforded.[24] Justice Harlan defines a twofold requirement that "a person must have exhibited an actual expectation of privacy and that the expectation be one that society is prepared to recognize as reasonable."[25] These subjective and objective prongs came a long way from leaving Congress to protect privacy[26] but still left many questions unanswered.

B. *Reasonableness*

Katz was able to address a majority of the "Five W's." People are

16. *Id.*; 18 U.S.C. § 1084 (1961).
17. *Katz*, 389 U.S. at 351.
18. *Id.*
19. *Id.* at 352.
20. *Id.*
21. *Id. at* 353.
22. *Id*. at 359.
23. 389 U.S. at 361 (Harlan, J., concurring).
24. *Id.* (The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.').
25. *Id.*
26. *See supra* text accompanying note 11.

protected by the Fourth Amendment, not places; although places may determine where a subjective and objective expectation is held. The Fourth Amendment's protections come into play when these subjective and objective expectations pertain to privacy and can be considered reasonable. A search can then be classified as something that violates the person when that person actually expects privacy and when society can recognize that expectation as reasonable. But this begs the question: what is reasonable?

Reasonable is defined as "having the faculty of reason and possessing sound judgment."[27] Society's sound judgment evolves over time. Consequently, courts have to emulate that modern sentiment in their decisions and continue to hear cases time and time again to address society's sound judgment. A plethora of issues since *Katz* have been addressed by various courts that were not problematic during 1967: if a legitimate expectation of privacy exists in specific areas of automobiles,[28] mobile homes,[29] open fields viewed from airplanes;[30] and if it is reasonable to search the automobile of someone after that person has been arrested outside of that vehicle.[31] In order to assist in making these decisions, courts came up with their own definitions to embody the term "reasonable" and an analysis of *Katz*:

> (1) Reasonableness consists of multiple factors: whether a person invoking the protection of the Fourth Amendment took normal precautions to maintain his privacy; the way a person has used a location; whether certain types of governmental intrusions historically were perceived to be objectionable; whether there are any attached property rights.[32]
> (2) A subjective expectation of privacy is reasonable "if a privacy expectation normally shared by people in that setting and it falls within some tolerance level which represents the limits of what

27. MERRIAM-WEBSTER (2014), *available at* http://www.merriam-webster.com/dictionary/reasonable.

28. Rakas v. Illinois, 439 U.S. 128 (1978) (determining that no legitimate expectation of privacy was found in the glove compartment or underneath a seat of a car).

29. California v. Carney, 471 U.S. 386 (1985) (holding that while it is possible that motor homes possess some, if not many, of the attributes of a home, it is equally clear that the vehicle falls clearly within the scope of the exception laid down in *Carroll* [search incident to arrest gives the right to search the person or anything in his control]).

30. United States v. DeBacker, 493 F. Supp. 1078, 1081 (1980) (holding that the viewing the open fields of marijuana from 50 feet above in an airplane was not a search).

31. New York v. Belton, 453 U.S. 454 (1981) (holding that when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile).

32. *Rakas*, 439 U.S. at 152.

society can accept given its interest in law enforcement."[33]
(3) Fourth Amendment analysis requires "assessing the nature of the particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[34]

As confident as these courts may have been in formulating or replicating reasonableness standards from precedent, some courts have declined to follow the interpretation set forth by others. This could be due to state law grounds and the shifting of the burden[35] or a declination to follow persuasive authority.[36] Accordingly, there lacks a definitive bright-line test that can be consistent along federal and state lines causing many courts to adopt *Katz* and still come to different holdings due to the "reasonableness" analysis.

C. *When is a Warrant Required?*

The Fourth Amendment contains two clauses: (1) the reasonableness clause ("[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated") and (2) the warrant clause ("no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized").[37] The U.S. Supreme Court in *Katz* decided to address both clauses. The two-fold requirement enunciated by Justice Harlan attempted to explain the reasonableness clause,[38] while one sentence articulated by the majority compiled precedent to explain the warrant clause: "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions."[39]

As precise as *Katz* made the warrant requirement sound, exceptions have begun to overshadow the rule. One exception is known as "exigent circumstances," an emergency situation requiring quick action to prevent imminent danger to life or serious damage to property, or to forestall the

33. United States v. Oliver, 657 F.2d 85, 87 (6th Cir. 1981).

34. *DeBacker*, 493 F. Supp. at 1081 (quoting United States v. White, 401 U.S. 745, 786 (1971) (Harland, J., dissenting)).

35. *See* State v. Brown, 83 A.3d 45 (N.J. 2014) (finding that their state constitution provides greater standing rights to individuals than the Fourth Amendment [of the U.S. Constitution].)

36. *See* United States v. Cherry, 876 F. Supp. 547 (S.D.N.Y 1995).

37. U.S. CONST. amend. IV.

38. *See supra* Part II.A.

39. Katz v. United States, 389 U.S. 347, 357 (1967).

imminent escape of a suspect or destruction of evidence.[40] Exigent circumstances have been recognized since at least 1948 in *Johnson v. United States*.[41] In *Johnson*, police received information from a confidential informant about unknown people smoking opium in a hotel at night.[42] Four agents arrived at the hotel to recognize a strong, distinct odor of opium coming out of a specific hotel room.[43] After knocking on the door, the occupants of the room shuffled around the room before opening the door.[44] The occupants let the police in and the police informed them that a search was going to occur.[45] The search uncovered opium and drug paraphernalia that was still warm.[46] The Supreme Court stated that there needed to be "exceptional circumstances" in which, on balancing the need for effective law enforcement against the right of privacy, a warrant will not be acquired ahead of time; this case was not an example of that.[47] The search took place in a permanent place and no evidence was threatened with being removed, except for potential fumes of opium.[48] Being inconvenienced in preparing and presenting evidence to a magistrate is no excuse for ignoring the constitutional duty.[49]

A second exception to the warrant requirement is a search incident to a lawful arrest. Approval of a warrantless search incident to a lawful arrest was first articulated by the Supreme Court in 1914 in *Weeks v. United States*.[50] According to *Weeks*, the search incident to arrest had always been recognized under both English and American law to discover and seize the fruits or evidences of crime.[51] This was interpreted as containing the search to just the 'person' being arrested. This expanded eleven years later to include whatever is found upon his person or in his control which may be used to prove the offense may be seized and held as evidence[52] and then several months later to include the place where the arrest is made.[53] Forty-four years later, the scope of a permissible search was narrowed to a mere search of the arrestee's person and only the area within his immediate control.[54]

---

40. People v. Ramey, 545 P.2d 1333, 1341 (Cal. 1976).
41. Johnson v. United States, 333 U.S. 10, 14-15 (1948).
42. *Id.* at 12.
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. 333 U.S. at 14-15.
48. *Id.* at 15.
49. *Id.*
50. 232 U.S. 383, 392 (1914).
51. *Id.*
52. Carroll v. United States, 267 U.S. 132, 158 (1925) (emphasis added).
53. Agnello v. United States, 269 U.S. 20, 29 (1925).
54. Chimel v. California, 395 U.S. 752, 763 (1969). The "area within [the arrestee's]

It was found to be reasonable for the arresting officer to "search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape" and "search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."[55] These two underlying codes became known as the two justifying principles for a search incident to arrest. The existence of these principles was evaluated on a case-by-case basis, until 1973 in *United States v. Robinson*.[56] *Robinson* attempted to create a bright-line rule to control consistency within the courts and avoid varying opinions. The Court acknowledged that no justification is even needed if a suspect is arrested based on probable cause; no unreasonable intrusion has occurred.[57] The scope of the search was broadened to include an automatic right to search containers on the arrestee.[58]

III. CELL PHONES AND THE FOURTH AMENDMENT

The first commercially available handheld cell phone was purchased for almost $4,000 over thirty years ago.[59] The revolutionary invention of the handheld phone began to bridge the spatial gap between people, making it easier to connect with someone from a distance. First conceptualized as a "'look what I got!' rich man's toy," the cell phone has now become one of the most ubiquitous gadgets in history.[60] As the Spider-man comics say it best, "with great power comes great responsibility."[61] This new handheld invention consequently led to complications when courts had to address any rights accompanying the new technology. The Court had to answer: how do cell phones fit into the scheme of the Fourth Amendment?

A. *Classification of Phones*

The Court in *Katz* acknowledged that the electronic device used to listen and record the defendant's words in the telephone booth violated

---

immediate control meant the area from within which he might gain possession of a weapon or destructible evidence." *Id.*

55. *Id. at* 762-63.

56. United States v. Robinson, 414 U.S. 218, 235 (1973).

57. *Id.*

58. *Id.*

59. Stewart Wolpin, *The First Cellphone Went on Sale 30 Years Ago for $4,000*, Mashable (Mar. 13, 2014), http://mashable.com/2014/03/13/first-cellphone-on-sale/.

60. *Id.*

61. The first adaptation of this quote appears in the AMAZING FANTASY NO. 15 released by Marvel Comics in 1962. http://en.wikiquote.org/wiki/Stan_Lee (last visited Nov. 14, 2014).

his privacy that he had justifiably relied on.[62] The thought of a "technical trespass" under property law evolved to include the electronic device since it achieved the same end result.[63] Approximately twelve years later, the Court addressed the issue of whether the government's use of a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released was considered a search.[64] The Court expressed doubt that people entertain any expectation of privacy in the numbers they dial since those numbers are being conveyed to a telephone company through switching equipment.[65] Using a *Katz* two-pronged analysis, the defendant's argument that a search had occurred failed.[66]

Moving away from the physical intrusion of trespass, courts seem to accept the ever-advancing quality of technology. In 1992, the Fifth Circuit in *United States v. Smith* stated:

> In any consideration of the "societal understanding" about the privacy expectations of cordless phone users, it is perhaps instructive to note the important role that all forms of telecommunication, including various cordless systems, play in today's society.
>
> . . .
>
> If, as some experts predict, we are moving inexorably toward a completely cordless telephone system, the decision as to whether cordless telephone conversations are protected by the Fourth Amendment may ultimately determine whether *any* telephone conversation is protected by the Fourth Amendment.[67]

The *Smith* Court noted that from a Fourth Amendment standpoint, the problem with cordless phones is figuring out how exactly to characterize them: are they more like traditional telephones or more like radio transmitters?[68] Radio transmitters are afforded no protection due to the analogous nature of carrying on a loud oral conversation while *Katz* held that land-based telephone lines were protected.[69] The *Smith* Court came to the conclusion the issue is not whether it is *conceivable* that someone could eavesdrop on a conversation but whether it is *reasonable* to expect

62. Katz v. United States, 389 U.S. 347, 353 (1967).
63. *Id.*
64. Smith v. Maryland, 442 U.S. 735, 735 n.1 (1979).
65. *Id.* at 742.
66. *Id.*
67. United States v. Smith, 978 F.2d 171, 177 (5th Cir. 1992).
68. *Id.*
69. *Id.* (citing United States v. Hall, 488 F.2d 193, 196 (9th Cir. 1973) as it pertains to radio transmissions.)

privacy in a given setting.[70] Application of the Fourth Amendment in any case will depend largely upon the specific technology used; as technology advances to cover a wider net of privacy, at some point the communication will be entitled to Fourth Amendment protection.[71]

Courts have since that time acknowledged that Fourth Amendment protections do attach to a defendant's cell phone.[72] This has resolved many questions dealing with a defendant's standing in bringing a motion to suppress a search of a cell phone.[73] But this leaves open the same issues that early Fourth Amendment cases dealt with, such as the developing societal opinion of what can be considered reasonable for a cell phone user and the application of exceptions to the warrant requirement.

B. *Reasonableness of Phones*

The *Katz* court makes it clear that a person's Fourth Amendment rights have been violated when a subjective and objective privacy expectation is reasonably held by that person.[74] What can be defined as reasonable by society is constantly open to interpretation and must be addressed by the courts. As cell phone use becomes so ubiquitous, society's understanding and expectation of privacy changes. The inconsistency of perceptions with respect to reasonableness of private cell phone use has caused courts to issue a series of opinions allowing some cell phone searches but not others.[75] These case specific holdings are in juxtaposition with the Supreme Court's insistence on bright-line rules in the Fourth Amendment context.[76] Before adopting a particular bright line test, the court should ask itself four questions:

> (1) Does the proposed rule have clear and certain boundaries, so that it in fact makes case-by-case evaluation and adjudication unnecessary?
> (2) Does it produce results approximating those which would be obtained *if* accurate case-by-case application of the underlying principle were practicable?
> (3) Is it responsive to a genuine need to forego case-by-case

70. *Id.* at 180.
71. *Id.*
72. *See, e.g.*, United States v. Gomez, 807 F. Supp. 2d 1134, 1140 (S.D. Fla. 2011).
73. Standing is the "the legally protectable stake or interest that an individual has in a dispute that entitles him to bring the controversy before the court to obtain judicial relief." THE FREE DICTIONARY, http://legal-dictionary.thefreedictionary.com/standing (last visited Nov. 15, 2014).
74. *See* Part II.B.
75. United States v. Wurie, 728 F.3d 1, 12 (1st Cir. 2013).
76. Thorton v. United States, 541 U.S. 615, 623 (2004).

application of a principle because that approach has proved unworkable?
(4) Is it not readily subject to manipulation and abuse?[77]

Commentators have pointed out that the protection of the Fourth and Fourteenth Amendments "can only be realized if the police are acting under a set of rules which, in most instances, makes it possible to reach a correct determination beforehand as to whether an invasion of privacy is justified in the interest of law enforcement."[78] Courts have attempted to come up with bright-line rules for cell phones by looking beyond the case at hand and theorizing about the long-term effects of the decision.[79] As Judge Howard stated, "for the Constitution is as durable as technology is disruptive. In this exercise, consistency is a virtue."[80] But making a bright-line rule to have clear and certain boundaries to produce accurate results may not be possible when the functions of a cell phone are progressing in ways that were unexpected even ten years ago.

Cell phones can provide a multitude of functions, ranging from making and receiving phones calls, storing information in an address book, providing location features, and sending and receiving text messages. All of these functions carry with them different forms of information carried by a single user with potentially varying levels of protection.

1. Identification Information

"Identification information" describes information that merely identifies parties to the communication without disclosing the subject matter of that communication. This would consist of phone numbers in a call log, information inputted into an address book for a contact (*i.e.*, names, numbers, addresses), and the list of recently received text messages. This information would not disclose the content of a communication between two people; but rather, just the observation of the identity of another party that could be communicating with the owner of the cell phone.

The main question to identification information would be whether an individual holds a reasonable expectation of privacy to this specific type of information stored onto his or her cell phone that society is prepared to recognize as reasonable. If there is a reasonable expectation of privacy

77. Wayne R. LaFave, *The Fourth Amendment In an Imperfect World: On Drawing "Bright Lines" and "Good Faith*," 43 U. PITT. L. REV. 307, 325-26 (1982).

78. Wayne R. LaFave, *"Case-By-Case Adjudication" Versus "Standardized Procedures": The Robinson Dilemma*, 1974 SUP. CT. REV. 127.

79. *Wurie*, 728 F.3d at 14 (Howard, J., dissenting).

80. *Id.*

in identification information held by both the owner and society, then an officer's intrusion into examining that information would violate the owner's Fourth Amendment right.

Earlier cases, when cell phones were beginning to be widely used, began by addressing questions of law enforcement answering an arrestee's cell phone without seeking consent and without a warrant.[81] *United States v. De La Paz* in 1999 established that an arrestee can have a legitimate privacy interest in the fact that calls were received and in the identity of the callers.[82] Before this time, no court had answered this question with respect to cell phones.[83] Conventional, land-line, telephones gave the arrestee far less of a legitimate expectation of privacy: none.[84] As long as the law enforcement officers were lawfully on the premises, they could answer a telephone there.[85] The Court singled out this rationale, stating that "it confuses the privacy interest invaded by a search alone with the interest in whatever is uncovered by a search."[86]

Early cell phones with limited uses—primarily identification information—can be compared more so to electronic pagers. In these cases, courts have consistently held that the owner of an electronic pager has a legitimate interest in the numerical codes transmitted to the device, even while in the government's possession.[87] But even the court in *De La Paz* noted "if anything, the argument for privacy is even greater in cases involving cellular telephones insofar as the information communicated is likely to be at once more significant and more personal than a numerical code."[88]

Eight years later, in 2007, the Fifth Circuit in *United States v. Finley* held that the law enforcement's retrieval of the call records and text messages of the defendant was lawful.[89] The court used Fourth Amendment precedent to come to this conclusion: a search incident to a lawful arrest is reasonable; police officers may look for evidence on the arrestee's person; and the permissible scope of a search incident to arrest can extend to containers found on the arrestee's person.[90] The defendant's cell phone was considered an effect seized from the defendant's person and "property not immediately associated with his person" because it was on him at the time of his arrest.[91] Cell phones, and the information

81. United States v. De La Paz, 43 F. Supp. 2d 370, 371 (S.D.N.Y. 1999).
82. *Id.* at 372.
83. *Id.* at 371.
84. *Id.*
85. *Id.*
86. *Id.* at 372.
87. *Id.* at 373.
88. *Id.*
89. United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007).
90. *Id.* at 259-60.
91. *Id.* n.7.

contained within, were garnering more legitimacy as a Fourth Amendment right afterwards due to this new categorization of being an "effect."[92]

Courts have used the reasoning of *De La Paz* and *Finley* to make the logical conclusion that an individual also has a reasonable expectation of privacy with respect to operational functions, such as making calls.[93] Further, courts have held that the defendant had a reasonable expectation of privacy in his cell phone as a whole.[94] However, by acknowledging that the cell phone fits into the scheme of the Fourth Amendment, the same exceptions to a warrant apply. In terms of operational functions, the Southern District of Florida has found that law enforcement was justified in searching a defendant's cell phone to review and record its recent call log history due to the fact that the phone was found within the defendant's reaching distance and a name on the caller ID was in plain view.[95]

Even though the courts acknowledge that identification information on a cell phone can be a legitimate privacy interest, these interests are not necessarily being protected. Both the *De La Paz* and *Finley* courts held that the officers could search the cell phones and did not violate the Fourth Amendment in doing so.[96] The privacy levels of the identification information seized seem to be the lowest among the types of information obtained by a cell phone due to the fact that not as much private information is shared. However, because the distinction is never made in the judicial system, it is hard to make a solid line of demarcation between the levels of protection with these different types of information.

2. Location Information

"Location information" describes information that can be obtained to determine the exact coordinates of a person's location. This would consist of real time cell site location information (CSLI), a function of the cell phone used by the government to identify the location of a phone at the present moment, and historical cell site information, constituting the records stored by a wireless service provider that detail the location of a cell phone in the past.[97] This information has the potential to divulge the

92. However, not all courts find that a cell phone is an "effect." In *United States v. Park*, the Northern District of California found that for purposes of Fourth Amendment analysis cellular phones should be considered "possessions within an arrestee's immediate control" due to the cell phone's capacity for storing immense amounts of private information. 2007 WL 1521573, at 8 (N.D. Cal. May 23, 2007).

93. United States v. Gomez, 807 F. Supp. 2d 1134, 1140 (S.D. Fla. 2011).

94. *Id.* at 1141 (emphasis added).

95. *Id.* at 1142, 1145.

96. United States v. De La Paz, 43 F. Supp. 2d 370, 375 (S.D.N.Y. 1999); *Finley*, 477 F.3d at 259.

97. Deborah F. Buckman, *Allowable Uses of Federal Pen Register and Trap and Trace*

precise latitude and longitude coordinates of the cell phone owner.

The courts seem to possess two different schools of thought about the use of the cell site location information by the government; something that still remains unanswered by the U.S. Supreme Court. The first can be summarized by *United States v. Skinner* in 2012:

> When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them.
>
> . . .
>
> The Constitution, however, does not protect their erroneous expectations regarding the undetectability of their modern tools.[98]

Skinner was one of the first courts to address this particular issue. In *Skinner*, the government used the cell site location data from the defendant's phone to determine its real-time location as he transported drugs along the public thoroughfares between Arizona and Tennessee.[99] Law enforcement used this information to locate the defendant at a rest stop with over 1100 pounds of marijuana.[100] The Court held that Mr. Skinner could have no reasonable expectation of privacy in the data given off by his cell phone, stating that the "law cannot be that a criminal is entitled to rely on the expected untrackability of his tools."[101]

This ideology is supported by the precedent of tracking a defendant using a strategically placed beeper.[102] The Supreme Court has held that this type of monitoring does not violate the Fourth Amendment because the surveillance amounted to following an automobile on public streets and highways.[103] There is no reasonable expectation of privacy from moving one place to another in this context.[104] Cell site information in this way could be obtained through visual surveillance if the government is tracking the defendant on public streets.[105] Another court noted that visual observation is possible by any member of the public; law enforcement just used the CSLI to augment the "sensory faculties bestowed upon them at birth."[106] A second argument in favor of this ideology would be that defendants are put on notice that disclosure of the

---

Device to Trace Cell Phones and Internet Use, 15 ALR Fed. 2d 537, 545 (2010).

98. United States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012).
99. *Id.*
100. *Id.*
101. *Id.* at 777.
102. *See* United States v. Knotts, 460 U.S. 276 (1983).
103. *Id.* at 281.
104. *Id.*
105. *See Skinner*, 690 F.3d at 778.
106. United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004).

CSLI to law enforcement may occur in an emergency, absolving that defendant of any reasonable expectation of privacy in that information.[107]

The second school of thought streams from the most recent case on this subject: *Tracey v. Florida*.[108] The Supreme Court of Florida recognized that technology has advanced to the point that a person's whereabouts can be ascertained easily and at a low cost by the government.[109] The court viewed the beeper cases quite differently, stating that the question was left open of the application of the Fourth Amendment to longer term surveillance and that tracking into a protected location violates the Fourth Amendment.[110] However, the length of the time the cell phone is monitored is not a workable analysis due to its case-by-case and after-the-fact nature.[111]

The Supreme Court has recognized protection of personal and societal values regarding expectation of privacy that a society is willing to recognize, even where such activities are not fully concealed.[112] The *Tracey* court applied this to CSLI, stating that "simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes . . . does not mean that the user is consenting to use that information . . . for any other unrelated purpose."[113] The second school of thought addresses the first school of thought, stating that it would be a fiction to believe that the American population consents to warrantless access to the records of their movements by choosing to carry a cell phone around.[114]

A cell phone user does have the capability to prevent CSLI from being used by the government by turning off the cell phone.[115] However, requiring users to perform that action to assure the privacy from governmental intrusion can place an unreasonable burden on the user to forego necessary use of their cell phones.[116] With nearly three-quarters of smart phone users reporting to be within five feet of their phones most of the time,[117] it seems as though upcoming courts will provide some protection to a cell phone users' location due to the growing societal expectation of privacy that accompanies it. However, there still remains the possibility of a resurgence of lesser protection from the possibility of

107. United States v. Caraballo, 963 F. Supp. 2d 341, 352 (D. Ver. 2013).
108. Tracey v. Florida, 152 So. 3d 504 (Fla. 2014).
109. *Id.* at 512.
110. *Id.* at 513.
111. *Id.* at 520.
112. *Id.* at 521 (citing California v. Ciraolo, 476 U.S. 207 (1986)).
113. *Id.*
114. *Id.* at 523.
115. *Id.*
116. *Id.*
117. *Id.* at 524.

visual surveillance. Until the Supreme Court addresses this issue, courts may remain divided.[118]

3. Content Information

"Content information" describes the subject matter of communication between parties, as well as privately stored data for personal use. This includes the substance of a voicemail, the actual text of text messages, the conversation transmitted in a phone call, the photographs contained on the cell phone, and any data used from the Internet or third party applications. As smartphones become more of a ubiquitous feature in people's lives, the courts are forced to address what privacy expectations have become more reasonable over time.

Courts have held that advancements in cell phone technology and the volume of information citizens can store on their cell phones is relevant to a Fourth Amendment analysis.[119] With the first ever text message being sent twenty-two years ago, billions of text messages are sent per year.[120] One of the first types of text messaging was accomplished through alphanumeric pagers.[121] Although outdated, the Ninth Circuit in 2008 addressed a case involving alphanumeric pagers and a police department's review of an employee's text messages.[122] The court held that the employee did have a reasonable expectation of privacy in his city-owned pager, even if the department's polices stated the opposite.[123] This was made in contrast to letters and emails, where it is not reasonable to expect privacy in the information used to "address" these types of communication ("identification information").[124] Although a member of the public could have requested the employee's text messages, the court analyzed, that does not make his belief in the privacy of the text messages objectively unreasonable.[125]

---

118. Federal courts have been divided on historical CSLI as well. Most of the division from this type of information stem from whether probable cause or simply specific and articulable facts are required for authorization to access such information. *Id.* at 9. Because this falls outside the topic of my paper, I chose not to address it.

119. United States v. Park, 2007 WL 1521573 (N.D. Cal. 2007).

120. *First Text Message Ever Sent 20 Years Ago* (Dec. 17, 2012), http://www.myfoxphilly.com/story/20248180/20-years-ago-today-first-text-message-sent.

121. Alphanumeric text-messaging pagers worked as follows: the message leaves the originating pager via a radio frequency transmission. That transmission is received by one of the receiving stations. Depending on the location of the receiving station, the message is then entered into the computer network either by wire transmission or satellite. The message is sent to the computer server and stored for a period of up to 72 hours. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 895-96 (9th Cir. 2008).

122. *Id.*

123. *Id* at 906.

124. *Id.* at 905.

125. *Id.* at 907-08.

While the Ninth Circuit stated that this was a "context-sensitive inquiry,"[126] other courts have also found that there is a reasonable expectation of privacy in the context of the text messages on a cell phone.[127] In *Finley*, law enforcement had searched through the text messages of Mr. Finley's cell phone, noting that several of the text messages appeared to be related to narcotics use and trafficking.[128] This appearance would not have been known had law enforcement not looked through the content of the text messages. The *Finley* court noted that even though this was an employer-owned phone, a person in Finley's position can reasonably expect to be free from intrusion even though the employer could have read the text messages.[129] Although many text message cases have not been addressed by the courts, it is clear that there is a larger intrusion into the content of a text message and the information it may reveal.

In addition, photographs contained within the cell phone, as opposed to pictures used as the wallpaper, are content information for which a cell phone user should have a reasonable expectation of privacy. A picture can display more private information than a text message can type. As the old adage says, "a picture is worth a thousand words." There has been a severe lack of cases dealing primarily with cell phone photographs. However, it has been arising in the context of searches incident to arrest and the scope of a search.[130]

An owner of a cell phone generally has a reasonable expectation of privacy in the electronic data stored on the phone.[131] Courts have recognized that a cell phone should be distinguished from a person's wallet, which could be used to confirm identity, and a briefcase, which could contain a weapon or destructible evidence.[132] In 2013, the Northern District of Georgia recognized that:

> Modern cell phones, like Defendant's Samsung, are in effect mini-computers, and contain contacts, text messages, photographs, calendars, notes and memos, instant messages, voice memos, and e-mail messages – a wealth of private information held within a small digital "container," as it were, but a different kind of container from a crumpled cigarette package or even a footlocker.
> . . .

126. *Id.* at 906.
127. United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007).
128. *Id.* at 254.
129. *Id.* at 259.
130. *See infra* Part III.C.
131. *Quon*, 529 F.3d at 905; United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009).
132. United States v. Dixon, 984 F. Supp. 2d 1347, 1352 (N.D. Ga. 2013).

> A cell phone is an integrated digital device that holds only data and digitally stored information.[133]

By noting the differences in what information a cell phone can hold, legitimate privacy interests of arrestee's cell phones could warrant far more protection. However, courts, including the U.S. Supreme Court, are hesitant to establish far-reaching premises that define the existence, and extent of privacy expectations enjoyed by people using communication devices.[134] The judiciary is concerned about elaborating too fully on Fourth Amendment implications of emerging technology before its role in society has become clear.[135] This is due to the fact that "[r]apid changes in the dynamics of communication and information transmission are evidence not just in the technology itself but in what society accepts as proper behavior."[136] Up until this past year, courts used a case-by-case basis to find certain aspects of cell phones to have a legitimate expectation of privacy, given the right set of facts.

C. *Warrant Exceptions with Cell Phones*

With legitimate expectations of privacy in cell phones being somewhat recognized, courts have had to address a second issue: whether the searches performed by law enforcement of the cell phones were unlawful. If an expectation of privacy was held by both the cell phone user and society recognized that expectation as being reasonable, then any violation of that expectation could constitute a search under the Fourth Amendment without a warrant. Courts have looked at the technical, advancing capabilities of cell phones while applying established, precedential exceptions to justify a search: exigent circumstances and searches incident to arrest.

As early as 2003, courts have been using the exigent circumstances exception to the warrant requirement and applying that to cell phones.[137] Recording the numbers of incoming phone calls stored in the cell phone's memory has been justified due to the "limited memory to store numbers."[138] In the event that subsequent incoming calls occurred, the earlier stored numbers could be overwritten or effectively deleted.[139] This was held to be a matter of exigency in order to prevent the destruction of

133. *Id.* at 1352-53.
134. City of Ontario, Cal. v. Quon, 560 U.S. 746, 759 (2010).
135. *Id.*
136. *Id.*
137. United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003).
138. *Id.* at 1303-04.
139. *Id.* at 1303.

evidence.[140]

Courts have used this rationale and applied it to the reasonable beliefs held by investigating law enforcement agents.[141] The functions and limitations of the cell phone technology are believed by law enforcement to be dynamic, subject to change without warning by a call simply being made to the phone.[142] Due to the risk of numbers being erased and the significant evidentiary value of these functions, agents can be motivated to conduct an immediate search of a cell phone.[143]

Multiple courts have concluded that the search incident to arrest exception must apply given certain facts to cell phones.[144] These courts reason that searches of highly personal items (*i.e.*, wallets or purses), which are analogous to electronic storage devices (*i.e.*, cell phones), are permissible if searched incident to arrest regardless of any exigent circumstance.[145] For this exception to apply, the only consequential matters are the location that the device was found incident to arrest and the time that the search was conducted.[146] By applying these two matters, a District Court in Florida has stated that:

> The scope of a search will be limited as a practical matter. In the case of a cell or smartphone, for instance, a search contemporaneous with an arrest would not possibly allow a law enforcement officer at the scene of an arrest from downloading the entire content of the phone's memory.[147]

This court held that a short, limited perusal of only recent calls to quickly determine if any incriminating evidence is relevant to the crime was permissible.[148] However, it is difficult to use this analysis when trying to estimate what goes beyond the requirements of the search incident to arrest and what falls within it. For example, when a defendant is arrested for drug-related activity, the police may be justified in searching the contents of the arrestee's cell phone for evidence related to the crime of the arrest, even if the presence of such evidence is improbable.[149] By having courts find cell phone users have an expectation of privacy in their electronic data on phones, a blurred line appears in the

---

140. *Id.* at 1304.

141. United States v. Zamora, 2006 WL 418390 (N.D. Ga. Feb. 21, 2006).

142. *Id.* at 4.

143. *Id.*

144. United States v. Gomez, 807 F. Supp. 2d 1134, 1146 (S.D. Fla. 2011); United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).

145. *Gomez*, 807 F. Supp. 2d at 1146.

146. *Id.* at 1148.

147. *Id.*

148. *Id.*

149. United States v. Quintana, 594 F. Supp. 2d 1291, 1291 (M.D. Fla. 2009).

reasonableness requirement of the Fourth Amendment.

IV. THE FUTURE OF SMARTPHONES

The future of the cell phone has been obvious: smartphones. A smartphone is a device that combines a cell phone with a hand-held computer, typically offering Internet access, data storage, e-mail capability, and other features beyond basic feature phones.[150] The technological capabilities of a smartphone far surpass any expectations that people could have had since the first handheld phone thirty years ago.[151] The ubiquitous nature of smartphones has diminished the price, making smartphones commercially available for every class of consumers. As the AT&T advertisements say, "AT&T has a smartphone for every budget!"[152]

A. Riley v. California

Due to the ever-growing availability and popularity of the smartphone, the U.S. Supreme Court finally addressed the question of a warrantless search of digital information on a cell phone in the summer of 2014.[153] This opinion consisted of two different cases. The first, petitioner Riley was stopped for a traffic violation that led to an arrest for possession of concealed firearms.[154] A law enforcement officer seized Riley's smartphone and accessed information on the phone leading to a belief that Riley was a member in a gang.[155] A detective specializing in gangs further went through Riley's phone for evidence because "gang members will often video themselves with guns or take pictures of themselves with guns."[156] The second, a police officer spotted petitioner Wurie making an apparent drug sale from a car.[157] After seizing Wurie's two "flip phones," phones that have a smaller range of features than a smartphone, police opened the phone, saw several photographs, accessed the call log, and traced a phone directory to trace the phone number listed as "my house" to an apartment building.[158]

---

150. DICTIONARY.COM, http://dictionary.reference.com/browse/ smartphone (last visited Nov. 19, 2014).

151. *See supra* text accompanying note 59.

152. AT&T, http://www.att.com/shop/wireless/devices/smartphones.html (last visited Nov. 19, 2014).

153. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

154. *Id.*

155. *Id.*

156. *Id.* at 2480-81.

157. *Id*. at 2481.

158. *Id.*

The Court made a revolutionary holding, one that addresses many issues and discrepancies that were left unresolved by lower courts. The holding was quite simple: a warrant is generally required before a search of the information on a cell phone is performed, even when that cell phone is seized incident to arrest.[159] The Court astutely recognized that:

> [Modern cell phones] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. 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.[160]

The scope of the search incident to arrest exception has been debated for as long as it has been recognized.[161] Since prior cases dealing with this exception have given vague guidelines, the Court choose to "assess, on 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" to determine the scope of a search incident to arrest as it would pertain to a cell phone.[162]

In assessing the government's legitimate interests, the Court found that a cell phone fails the two traditional justifying principles for a search incident to arrest: digital data cannot be used as a weapon or an escape and the destruction of evidence on the phone can be reasonably responded to.[163]

Most importantly, the Court recognized the vast privacy interests that would be at stake from a search of cell phone data. Even though an arrestee has a diminished interest in privacy that does not mean that the arrestee is not guaranteed his Fourth Amendment rights.[164] With this realization, the Court was finally able to address the fact that a cell phone is so much more than just a physical object; it contains vast quantities of personal information and places that quite literally into the hands of the cell phone user.[165] Sixteen gigabytes of storage, the most current top-selling and standard capacity in a smartphone, translates to millions of pages of text, thousands of pictures, or hundreds of videos.[166] Therefore, modern cell phones implicate privacy concerns far beyond those implicated by physical items found on an arrestee.[167]

---

159. *Id.* at 2484.
160. *Id.*
161. *Id.*; *see* Part II.C.
162. *Riley*, 134 S. Ct. at 2484.
163. *See id.* at 2485-88.
164. *Id.* at 2488.
165. *Id.* at 2485.
166. *Id.* at 2489.
167. *Id.* at 2488-89 ("Modern cell phones, as a category, implicate privacy concerns far

The Court even went so far as to identify several interrelated consequences for privacy for cell phone searches, such as collecting different types of information (identification, location, and content) all in one place; having the capacity to convey even more information than historically possible; and preserving information since at least the purchase of the phone.[168] Because it is now the rule, not the exception, to find a person carrying a cell phone complete with sensitive personal information, allowing the police to scrutinize this information on a daily basis would be drastically different than searching any other personal item or performing an exhaustive search of a house.[169]

The *Riley* Court made great strides when it comes to privacy in cell phones; however, problems remain. Although historically cases have recognized that the warrant requirement is "an important working part of our machinery of government" and not merely an inconvenience to law enforcement,[170] the *Riley* Court restricted the warrant requirement of a cell phone to be when a cell phone is *seized incident to arrest*.[171] Many exceptions to the warrant requirement remain, with the most important of them being exigent circumstances.[172] Exigent circumstances give law enforcement a fact-specific way to bypass the warrant requirement. So, the *Riley* Court's holding still leaves open a multitude of ways to search an arrestee's cell phone while not obtaining a warrant prior to doing so.

Exigent circumstances represent the antithesis of what the Court claims to want to establish for the Fourth Amendment: bright-line rules for police to enforce readily and reasonably.[173] The Court thought that by deterring warrantless searches of cell phones incident to arrest, privacy would be heightened and law enforcement would be negatively impacted.[174] Privacy is only heightened in this scenario if law enforcement, who under the facts and circumstances, does not believe that a reasonable person would conclude that either an offense was committed or a search could be done—as per the requirement of probable cause. All law enforcement now needs, instead of no justification for a search incident to arrest beyond probable cause for the arrest, is to be able to fit the search into one of three categories: (1) prevention of the imminent destruction of evidence; (2) pursuing a fleeing suspect; or (3) assisting persons who are seriously injured or are threatened with

---

beyond those implicated by the search of a cigarette pack, a wallet, or a purse.").

168. *Id.* at 2489.

169. *Id.* at 2490, 2491.

170. *Id.* at 2494.

171. *See supra* text accompanying note 159.

172. *See* Part II.C.

173. *See* Part III.B.

174. *Riley*, 134 S. Ct. at 2493.

imminent injury.[175] By leaving this exception open for wide use among law enforcement, the Court has created a large potential for abuse and a great avenue for law enforcement to get clever in their reasoning behind searches.

The *Riley* Court gives two unreasonable examples of what could be considered an exigent circumstance as it pertains to cell phones. The first was "a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb" and the second "a child abductor who may have information about the child's location on his cell phone."[176] Society would not recognize any expectation of privacy in those types of uncommon scenarios, making them unreasonable and unprotected. This begs the question: what about reasonable scenarios that could fit the exigent circumstance exception for the most common of crimes?[177] Examples of this could be: a person burglarizing a home and filming it with his cell phone; a person looking into the screen of his cell phone when he is trespassing; and a person talking on his cell phone whilst stealing items and viewed by law enforcement.

Would law enforcement then be able to search any information on a person's cell phone when that person is simply looking at it because there is a potential that the person is either destroying information or injuring others? The *Riley* Court fails to draw any sort of line as to what law enforcement can or cannot do using the exigent circumstance exception. Even in the *Riley* Court's first example, how would law enforcement know that the suspect is texting an accomplice without going into the identification information of his cell phone? Furthermore, how would law enforcement know the subject of their communications without going into the content information of his cell phone? There is no way to know how many different types of information may be left open to search once one of the three rationales for the exigent circumstance exception is suspected by a police officer. The question then becomes: did the *Riley* Court promote privacy interests of individuals or diminish them?

B. *Fifth Amendment Concerns*

As smartphones advance in memory storage and contain more private information, cell phone companies invent ways to make it more difficult for an uninvited third party to access that information. Two of these security measures are available on several smartphones: passcodes and

175. *Id.* at 2494.

176. *Id.*

177. As of April 2013, the most common crimes in the United States were property crimes, as opposed to violent crimes. These would include: larceny/theft, burglary, motor vehicle theft, and robbery. CRIMINAL JUSTICE DEGREE HUB, http://www.criminaljusticedegreehub.com/what-are-the-most-common-crimes-in-the-united-states/ (last visited Nov. 21, 2014).

fingerprint readers. A passcode is typically a simple four-digit code but can be set to be more complex by the cell phone user.[178] It is meant to be an option to create a "barrier" between information on the user's device and someone else trying to access it.[179] Apple released Touch ID, a fingerprint reader in a cell phone user's handset that allows the operating system to unlock certain functionality features when the user touches the home screen.[180] Because the vast majority of cell phone users never lock their phones with a passcode, Touch ID was meant to replace the passcode and rid the user of memorizing a series of numbers and letters.[181]

The Fifth Amendment states: "No person shall . . . be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."[182] For the privilege against self-incrimination to apply, the information sought must be incriminating, personal to the defendant, obtained by compulsion, and testimonial or communicative in nature.[183] Courts have rarely looked at how gaining access to technology can implicate the Fifth Amendment. In one of the rare cases, a District Court in 2010 addressed whether requiring the defendant to provide the password to his computer was a testimonial communication.[184] The defendant in this case was issued a subpoena to produce the password to his computer in order for a grand jury to obtain evidence of child pornography.[185] The court found that forcing the defendant to reveal the password for the computer communicates a factual assertion to the government; it requires the defendant to communicate "knowledge."[186] Ultimately, this would require the defendant to divulge through his mental processes for something that will be used to incriminate him.[187]

Although this case did not directly deal with cell phones, smartphones combine both a cell phone and a computer.[188] A password to get into a

178. *Manage Your Privacy*, APPLE, https://www.apple.com/privacy/manage-your-privacy/ (last visited Dec. 3, 2014).

179. *Id.*

180. Marco Tabini, *Open Sesame: How iOS 8 Will Unlock Touch ID's Power*, MACWORLD (July 22, 2014, 5:00 AM), http://www.macworld.com/article/2455474/open-sesame-how-ios-8-will-unlock-touch-ids-power.html.

181. *Id.*

182. *Amendment V*, NATIONAL CONSTITUTION CENTER, http://constitutioncenter.org/constitution/the-amendments/amendment-5-trial-and-punishment-compensation-for-takings.

183. Izazaga v. Superior Court, 815 P.2d 304, 310 (Cal. 1991).

184. United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010).

185. *Id.* at 667.

186. *Id.* at 669.

187. *Id.*

188. *See supra* text accompanying note 150.

computer is reminiscent of a passcode for a smartphone, something meant to act as a barrier between the information contained within and outsider's access to it. But courts are still weary as to how to approach the capabilities of a smartphone—should it be distinguished from a computer and viewed according to an analysis of its particular functions or should smartphones now be considered a mini-computer?

One Virginia Beach Circuit Court judge has ruled in favor of the former.[189] In that case, the defendant, charged with Strangling another Causing Wounding or Injury, maintained a recording device that continuously recorded in the room where the assault was claimed to have taken place.[190] This recording device transmitted automatically to the defendant's smartphone, which was encrypted by either passcode or fingerprint.[191] The court had to resolve whether granting a motion to compel the production of the passcode or fingerprint would require "compulsion of a testimonial communication that is incriminating."[192] This required a two-fold analysis of testimonial communication by the court: one for passcodes and one for fingerprints.

The Circuit Court held that the defendant cannot be compelled to produce his passcode to access his smartphone, but could be compelled to produce his fingerprint.[193] Compelling the defendant to provide access through his passcode is both compelled and testimonial; it would be protected under the Fifth Amendment privilege.[194] A passcode is an invention of the defendant's mind, not known to any other person, according to the court.[195] It consists solely of mental processes. A fingerprint, on the other hand,[196] is similar to a key and does not require the defendant to communicate any information through his mental processes.[197] Therefore, the physical characteristics of the fingerprint make its compelled production non-testimonial.[198]

Although this passcode versus fingerprint distinction was determined in a Virginia Beach Circuit Court and is not binding on many jurisdictions, it can still be utilized as persuasive authority for other courts to draw on. Experts have been warning the population of the risk of fingerprint technology, such as Touch ID, as being legally unprotected.[199]

---

189. Commonwealth of Virginia v. Baust, No. CR14-1439 (Va. Cir. Ct. 2014), *available at* http://hamptonroads.com/2014/10/police-can-require-cellphone-fingerprint-not-pass-code.

190. *Id.* at 1.

191. *Id.* at 1-2.

192. *Id.* at 2.

193. *Id.* at 4.

194. *Id*. at 5.

195. *Baust*, *supra* note 189, at 5.

196. No pun intended.

197. *Baust*, *supra* note 189, at 5.

198. *See id*.

199. Lorenzo Francheschi-Bicchierai, *Cops Can Make You Unlocked Your Smartphone*

Since the Supreme Court has ruled in the past that the Fifth Amendment offers no protection against compulsion to submit to fingerprinting,[200] it is likely that many courts will follow suit with the Virginia Beach opinion.

The Fifth Amendment may also be used as a shield, instead of a sword, for the protection of a cell phone's contents. Widespread acceptance of constant, and sometimes dangerous, cell phone use has caused states to pass "distracted driving laws."[201] Distracted driving laws include cell phone use by novices, cell phone use by school bus drivers, text messaging, and handheld phones in general for all drivers. Washington was the first state to pass a ban on text messaging in 2007; since then, forty-five states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands ban text messaging for all drivers.[202] Fourteen states prohibit *all* drivers from using handheld cell phones while driving.[203] If found to be violating these laws, a law enforcement officer may cite a driver for using a handheld cell phone without any other traffic offense taking place.[204] More focus on the private use of cell phones means that law enforcement officers will be able to interact with people about their cell phone use.

Although *Riley* made it clear that the police cannot look through a person's cell phone text messages without a warrant,[205] the "distracted driving laws" make it a crime to do something using the functions of the cell phone to create content information. According to North Carolina's texting while driving statute:

> It shall be unlawful for any person to operate a vehicle on a public street or highway or public vehicular area while using a mobile telephone to:
> (1) Manually enter multiple letters or text in the device as a means of communicating with another person; or
> (2) Read any electronic mail or text message transmitted to the device or stored within the device, provided that this prohibition shall not apply to any name or number stored in the device nor to any caller identification information.[206]

Without Fingerprint, Says Judge, MASHABLE (Oct. 30, 2014), http://mashable.com/2014/10/30/cops-can-force-you-to-unlock-phone-with-fingerprint-ruling/.

200. Schmerber v. California, 384 U.S. 757, 764 (1966).

201. GOVERNORS HIGHWAY SAFETY ASSOCIATION, http://www.ghsa.org/html/stateinfo/laws/cellphone_laws.html (last visited Apr. 6, 2015).

202. *Id.*

203. *Id.*

204. *Id.*

205. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

206. N.C.G.S.A. § 20-137.4A (2012).

The main way a person can get ticketed for this offense would be to respond to the police officer's question when she asks "were you texting and driving?" After the *Riley* opinion, people pulled over for texting while driving now have the option to exercise their Fifth Amendment right. In response to the question "were you texting and driving," a North Carolina law firm now suggests that the suspect of a crime state "I'm going to exercise my Fifth Amendment right against self-incrimination" and never consent to a search of a cell phone.[207] The Lancaster Law Firm recommends a similar path for using the Fifth Amendment to prevent a suspect from being charged with or convicted of a violation of the texting law.[208] The firm states that the Fifth Amendment can be used in two methods: first, the actual cell phone can be a record of words or admissions that were made prior to the stop by law enforcement; second, is to place a password lock on the phone so that if law enforcement demands the password to the phone, then the police have asked the suspect to incriminate herself.[209] With this Fifth Amendment option ready to use it is not a mystery why enforcement of the law remains difficult.[210]

V. CONCLUSION

As technology advances, courts are expected to have answers for every new question. This constant expansion of jurisprudence can be difficult to apply to these new scenarios when such technology may not have been thought about even a year prior. What may be even more difficult to determine is society's reactions to these advances: what society now considers reasonable changes even more frequently than the technology does.

The landmark case of *Katz v. United States* declined to recognize the Fourth Amendment as a general right to privacy.[211] The Court stated:

> [The Fourth] Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go

---

207. John Scarbrough, *The Supreme Court's "Cell Phone" Case: The End of the "Texting While Driving" Ticket?*, Ferguson, Scarbrough, Hayes, Hawkins & Demay, PLLC (June 28, 2014), http://www.fspa.net/the-supreme-courts-cell-phone-case-the-end-of-the-texting-while-driving-ticket/.

208. LANCASTER LAW FIRM, http://www.thelancasterlawfirm.com/blog/criminal-law-blog/crim-law-texting-while-driving-and-the-fifth-amendment/ (last visited Apr. 6, 2015).

209. *Id.*

210. *See generally* Leith Ford, *Texting While Driving in North Carolina: Why the Law is Broken*, NEWS & RESEARCH FROM LEITH FORD (Aug. 6, 2014), http://www.leithford.com/blogs/660/texting-driving-north-carolina-law-broken/.

211. Katz v. United States, 389 U.S. 347, 350 (1967).

> further . . . But the protection of a person's general right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States.[212]

This refusal to recognize a general right to privacy has avoided the bright-line rules in the Fourth Amendment context that the Supreme Court insists upon. *Katz* led to a spiral of fact-specific holdings and multiple interpretations of the same words. Most courts seemed to find expectations reasonable through a balancing test: what society is prepared to recognize as a reasonable expectation of privacy versus the utility of exposing that privacy for security purposes. Although privacy was always a major concern among the courts, it was able to get pushed aside when a larger concern became more apparent.

One of these large concerns was how law enforcement could bypass the warrant requirement, something that is required by the Fourth Amendment. This requirement was overshadowed by two main exceptions, the search incident to arrest and exigent circumstances. These exceptions were created with either officer's safety, society's safety, or evidence's safety in mind; however, this diminished the immediate privacy attached to whatever was going to be searched.

As times changed, such as they have now with technology that has provided the government with technological capabilities scarcely imagined four decades ago, the protections of the Fourth Amendment have grown to be more, not less important.[213] This is especially true with the adaptation of cell phones to the modern world. Cell phones carry a wealth of information available in a tiny, portable device. Identification information shows the basic information present; location information displays the setting; and content information gives the subject. Society's expectation of privacy is likely to differ depending on the categorization of the information, with identification information being the least private and content information being the most private. However, courts struggle by not making this distinction; normally any of the privacy interests at stake will be overshadowed by the exception that the search is conducted under.

Newer models of cell phones are generally smartphones, a cell phone and computer hybrid that is capable of holding a vast amount of differing information. The *Riley* Court made great strides when it came to protecting privacy in smartphones, stating that police must get a warrant before searching a cell phone seized incident to an arrest.[214] However, that opinion left open the exigent circumstances exception to be used and

212. *Id.* at 350-51.

213. *Tracey*, 30 Fla. L. Weekly S617, at 6 (Fla. Oct. 16, 2014).

214. Riley v. California, 134 S. Ct. 2473, 2495 (2014).

abused by law enforcement. Since cell phones can sometimes be hard to classify as objects external from the human body,[215] law enforcement may be able to use any exigent circumstance rationale to be able to search the data of a cell phone without a warrant—something the *Riley* Court wanted to avoid.

Courts have disagreed on how to define a smartphone: should a smartphone be considered a computer or its own individual entity? The Supreme Court in *Riley* noted the quantitative and qualitative difference in smartphones, stating that "many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[216] Contrasted with the Supreme Court of Ohio holding that because cell phones now have a wide variety of functions, it would not be helpful to create a rule that would require officers to differentiate the capabilities of cell phones before they could act.[217]

A smartphone goes beyond the normal functioning of a container found on the arrestee's person. If a smartphone is viewed as more of a minicomputer, as the *Riley* Court has stated, then the scope of privacy interests widen dramatically.[218] The data a user views on smartphones may not be stored on the device itself but rather on remote servers using cloud computing.[219] Access to this information may provide access far beyond the particular cell phone user's "papers and effects" and into a whole new domain. The Supreme Court is going to need to address this issue in the context of the "third party doctrine" established in *Smith v. Maryland*, which states if a party knowingly exposes information to a third party and that party betrays them, there can be no claim of a Fourth Amendment violation.[220] Do smartphone users that store their information in the cloud assume the risk that information will be given up? Does society recognize that as reasonable?

Distinctions remain important in how law enforcement may compel access into a user's smartphone. According to a Virginia Beach Circuit Court, a passcode actually protects a smartphone, while the made-to-be-easy fingerprint reader endangers it.[221] Before this issue reaches the Supreme Court, states are going to be divisive in how they approach accessing a smartphone and defining what is testimonial.

Due to the lag of time in between state courts hearing a case and the Supreme Court granting certiari, privacy interests will consistently be on the verge of collapse unless courts seek to uphold basic constitutional

215. *See* text accompanying note 160.
216. *Riley*, 134 S. Ct. at 2489.
217. State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).
218. *See*, *e.g.*, *Riley*, 134 S. Ct. at 2491.
219. *Id.*
220. Smith v. Maryland, 442 U.S. 735 (1979).
221. *See supra* text accompanying notes 189-98.

guarantees—guarding against the potential for widespread intrusion into the privacy of individuals. The Supreme Court needs to answer these advancing technological questions by creating workable tests that can be applied to the different functioning features of a cell phone. Until this is done, exceptions for protection may dominate any requirements set forth and privacy interests may be without any protective limits.