:o OMG THEY SEARCHED MY TXTS: UNRAVELING THE SEARCH AND SEIZURE OF TEXT MESSAGES

KATHARINE M. O'CONNOR*

With billions sent each month, more and more Americans are using text messages to communicate with each other. Yet when it comes to protecting the privacy of these messages, courts, legislators, and commentators have struggled to apply outdated statutes and common law doctrine to the realities of this new technology. Exploring the ever-present tension between privacy concerns and law enforcement tactics, this Note examines the privacy issues presented by text messaging technology, focusing on the ability of criminal defendants to suppress text messages seized without warrants.

The author begins by briefly describing the technology behind text messaging and then outlines the statutory protections Congress has given electronic communications. The Note then turns to the Supreme Court, describing the relevant Fourth Amendment doctrine that the Court has developed and noting the different standards that have been applied to the search and seizure of oral communications, letters, and containers. The author next analyzes how the lower courts have tried to fit searches of text messages into these frameworks, noting the insufficiency of statutory protections and the inconsistencies that occur when courts analogize searches of cell phones to searches of containers or the seizure of text messages to the seizure of letters. The author argues that text messages are best analogized to spoken, rather than written, communications and presents a test based on the plain view doctrine that would allow law enforcement officers to seize and search a cell phone if they have probable cause to believe that it contains evidence of a crime. The author recommends the adoption of this probable cause approach, arguing that it provides the best balance between a cell phone user's privacy interests and the interests of law enforcement.

I. INTRODUCTION

In season five of the HBO television series *The Wire*, drug kingpin Marlo Stanfield's suppliers introduce a new way to communicate—coded

* J.D. Candidate 2010, University of Illinois College of Law. Many thanks to my friends and family for their support, especially Joni O'Connor, Michael O'Connor, and Jeffrey Freeman. Thanks as well to the *University of Illinois Law Review* administrative staff and my notes editors Christine Holst and Katie O'Brien.

photo messages sent via cell phone, known as "pix" messages.[1] In previous seasons of *The Wire*, the police succeeded in using a wiretap to build a case against Stanfield's predecessor, Avon Barksdale.[2] After Barksdale went to prison, Stanfield's crew rose to the top, careful to avoid using phones altogether.[3] After eventually cracking the pix message code, the police arrested Stanfield and seized the crew's phones; they then immediately sought search warrants to gain access to the phones' incriminating evidence.[4]

Criminal law issues surrounding the search and seizure of text and pix messages are not merely a figment of a few television writers' imaginations. In the recent scandal ending in Detroit Mayor Kwame Kilpatrick's resignation, *The Detroit Free Press* obtained text message transcripts from the city's cell phone provider implicating an affair between Kilpatrick and his chief of staff that proved both had lied under oath.[5] As a result of this discovery, Kilpatrick pled guilty to obstruction of justice charges.[6]

The Supreme Court of the United States has been addressing the intersection between telephones and the Fourth Amendment for more than eighty years.[7] The current test of what constitutes a Fourth Amendment search, in fact, derives from a case involving a defendant who was using a telephone booth to communicate illegal wagering information.[8] Cases involving telephones often highlight a perpetual tension in Fourth Amendment jurisprudence between privacy concerns and effective law enforcement tactics. This tension is evident in Justice Marshall's dissent in *Smith v. Maryland*, a case contesting the validity of pen register devices to track a phone user's calls.[9] In its decision, the Court distinguished the phone number from the conversation, maintaining that a dialer's conversations may have Fourth Amendment protections while the phone numbers dialed do not.[10] Justice Marshall

1. *The Wire: React Quotes* (HBO television broadcast Feb. 3, 2008).

2. *The Wire: Middle Ground* (HBO television broadcast Dec. 12, 2004).

3. *Id.*

4. *The Wire: Late Editions* (HBO television broadcast Mar. 2, 2008).

5. Jim Schaeffer & M. L. Elrick, *Mayor Lied Under Oath, Text Messages Show*, DETROIT FREE PRESS, Jan. 24, 2008, at 1A.

6. Jim Schaeffer et al., *'I Lied': Mayor Admits Guilt, Resigns from Office*, DETROIT FREE PRESS, Sept. 5, 2008, at 1S.

7. *Olmstead v. United States*, a Supreme Court case that formed the basis for the Court's jurisprudence regarding wiretaps until 1967, was decided in 1928. 277 U.S. 438 (1928).

8. Katz v. United States, 389 U.S. 347, 348 (1967).

9. Smith v. Maryland, 442 U.S. 735, 748 (1979) (Marshall, J., dissenting). The Court in *Smith* held that the Fourth Amendment does not prohibit the government's use of a pen register device without a warrant because an individual has no legitimate expectation of privacy in the phone numbers dialed. *Id.* at 745–46 (majority opinion). A pen register records only the numbers dialed. It differs from a wiretap because it does not record any part of the conversation and is usually installed at the telephone company's central offices. *Id.* at 736 n.1.

10. *Id.* at 743 ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

criticized the view that someone can "assume the risk" of exposing information to the police by the mere use of a certain technology.[11]

Marshall's concern that the majority's decision would diminish individual privacy exemplifies a strong tension in contemporary Fourth Amendment jurisprudence. A majority of the Court prefers bright-line rules easily applied by the police in the field.[12] The "popular view," on the other hand, espoused by Justice Marshall and subsequent legal scholars,[13] is that bright-line rules permit an increasing encroachment on individual privacy.[14]

Recent technological advances have spurred new discussions regarding the intersection between telephones and the Fourth Amendment. The frequency of text messaging in the United States has increased more than tenfold in the last five years, with more than 75 billion text messages sent per month in 2008.[15] As cellular phones are increasingly used to transport nonspoken communications, lower courts must decide how to treat this technology. Although few courts have faced the issue, most have viewed text and other written messages stored on wireless devices as analogous to the contents of a container[16]—applying the corresponding Supreme Court rules—this Note proposes a different analysis.

Part II begins by briefly describing the mechanism by which text messages are transmitted. It then describes the existing legislation regarding electronic communications, the Stored Communications Act, and the relevant Fourth Amendment jurisprudential background. Part III first analyzes the ineffectiveness of the Stored Communications Act in dealing with text messages, especially in the context of criminal cases. Next, it discusses three ways courts could view text messages under current Fourth Amendment jurisprudence: as written communications anal-

11. *Id.* at 749 (Marshall, J., dissenting).

12. *See, e.g.*, Thornton v. United States, 541 U.S. 615, 623 (2004) (permitting a search incident to arrest of an arrestee's car even though he has already exited and walked away from the car); United States v. Belton, 453 U.S. 454, 460 (1981) (allowing officers to search the passenger compartment of a car incident to a lawful arrest).

13. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 804 (2004) (stating that leading legal theorists support a broad interpretation of the Fourth Amendment in response to changing technology).

14. *See id.* The Court's recent decision in *Arizona v. Gant*, 129 S. Ct. 1710 (2009), demonstrates a retreat from the bright-line approach, however. Therefore, the "popular view" may even be the Court's view after *Gant*, discussed *infra* notes 110–17 and accompanying text.

15. Jennifer Steinhauer & Laura M. Holson, *Cellular Alert: As Texts Fly, Danger Lurks*, N.Y. TIMES, Sept. 20, 2008, at A1.

16. *See, e.g.*, United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007); United States v. Chan, 830 F. Supp. 531, 533 (N.D. Cal. 1993); State v. Novicky, No. A07-0170, 2008 WL 1747805, at *6 (Minn. Ct. App. Apr. 15, 2008) (accepting the container analogy without discussion). Interestingly, in one of the earlier cases involving pagers, Chan conceded that his pager was a container in order to argue that he had a reasonable expectation of privacy in the contents. *Chan*, 830 F. Supp. at 533. Since then, courts have expanded this analogy to messages on cell phones virtually without question. *But see* State v. Smith, No. 2008-1781, 2009 WL 4826991, at *4 (Ohio Dec. 15, 2009) (holding that a cell phone is not analogous to a closed container because it does not "have a physical object within it" and "stor[es] a wealth of digitized information").

ogous to letters, as the contents of a container, or as oral communications analogous to telephone conversations. In Part IV, the Note recommends that analogizing text messages to spoken communications best ensures a balance between individual privacy concerns and effective law enforcement. Finally, it recommends a new standard for text messages searches and seizures—the probable cause standard as applied in the plain view doctrine.

II. BACKGROUND

This Part gives the relevant background for analyzing the search and seizure of text messages by discussing the technology, the relevant statutory context, and the governing constitutional doctrines. This Part first describes how text messages are transmitted, which is relevant insofar as the courts rely on the mode of transmission to determine a sender's reasonable expectation of privacy. Next, it briefly describes the basic characteristics of the Stored Communications Act, the current federal statute protecting the privacy of electronic communications. Finally, this Part outlines the Fourth Amendment rules lower federal and state courts have applied in the text message context.

A. How Text Messages Work

Short Message Service (SMS) text messaging allows users to communicate between mobile phones or text-enabled pagers using written, as opposed to oral, communications.[17] The sender initiates a message by entering it into a mobile device and sending it.[18] The message is transmitted to a Short Message Center (SMC), where it is stored temporarily.[19] The SMC then forwards the message to the recipient's mobile device.[20] If the receiving device is unavailable, the SMC queues the message and attempts to send it again.[21]

In the realm of Fourth Amendment jurisprudence, one's legitimate expectation of privacy often depends on whether a third party has access to a communication and whether a communication has been received.[22] A sent message can be stored in at least two mobile devices: the sender's phone and the recipient's phone.[23] The message remains until a user deletes it, or it is deleted automatically to make way for new incoming mes-

17. Puneet Gupta, *Short Message Service: What, How and Where?*, WIRELESS DEVELOPER NETWORK, http://www.wirelessdevnet.com/channels/sms/features/sms.html (last visited Jan. 28, 2010).

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

22. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1978); *Ex parte* Jackson, 96 U.S. 727, 733, 735 (1878).

23. *See* Gupta, *supra* note 17.

sages.[24] The service provider may also store copies of messages on its server.[25] Therefore, the information in each text message is exposed to the following four places: (1) the SMC, (2) the service provider's network, (3) the sender's phone or wireless device, and (4) the recipient's phone or wireless device. That number increases exponentially for each additional recipient or, with the advent of new technology, as the message is forwarded to other users.

B. The Stored Communications Act

Congress already regulates access to electronic communications with the intended purpose of protecting the user's privacy. In 1986, Congress enacted the Stored Communications Act (SCA)[26] as part of the Electronic Communications Privacy Act (ECPA).[27] The ECPA's stated purpose is to protect the privacy of electronic information, particularly in light of the Fourth Amendment's inadequacies.[28] To enhance privacy protections, the SCA divides service providers into two now out-of-date categories: electronic communication services (ECS) and remote computing services (RCS).[29]

---

24. Some phones also delete messages automatically after a certain amount of time; for instance, a phone may automatically delete old messages when its memory is full, or a phone may be programmed to delete messages after the inbox reaches a certain capacity. *See, e.g.*, State v. Smith, No. 07-CA-47, 2008 WL 2861693, at *8 (Ohio Ct. App. July 25, 2008) (Fain, J., concurring). The prospect of losing text messages is becoming increasingly unlikely with new technology. The average text message is only 300 bytes, whereas the latest iPhone has a 32 gigabyte hard drive. Email from Bob Azzi, Senior Vice President, Network Services, Sprint-Nextel Corp., to Mike Azzi, Student, Univ. of Ill. College of Law (Nov. 30, 2009, 09:45 CST) (on file with author); Apple, iPhone—Technical Specifications, http://www.apple.com/iphone/specs.html (last visited Jan. 28, 2010). Additionally, new applications allow phone users to back up text messages on a computer. *See, e.g.*, Menoob.com, How to Save and Read Your iPhone Text Messages on Your Computer, http://menoob.com/iphone/how-to-save-and-read-your-iphone-text-messages-on-your-computer/ (last visited Jan. 28, 2010). As a result, users now have the capacity to save text messages indefinitely.

25. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 896 (9th Cir. 2008) (discussing the search of a service provider's records). Note that the Supreme Court recently granted certiorari on this case. *See id.*, *cert. granted sub. nom.* City of Ontario, Cal. v. Quon, No. 08-1332, 2009 WL 1146443, at *1 (U.S. Dec. 14, 2009). The Court's ultimate decision in this case is unlikely to affect the conclusion of this Note, as *Quon* deals with texting on employer-issued devices.

26. 18 U.S.C. §§ 2701–2712 (2006).

27. *Id.* §§ 2510–2712. The ECPA consists of three parts: (1) the Wiretap Act regulating information transmitted in real time, (2) the Stored Communications Act regulating information stored on servers and in databases, and (3) the Pen Register Act regulating "envelope" data. Alexander Díaz Morgan, Note, *A Broadened View of Privacy as a Check Against Government Access to E-Mail in the United States and the United Kingdom*, 40 N.Y.U. J. INT'L L. & POL. 803, 808–09 (2008).

28. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–10 (2004); Mikah K. Story, *Twenty-First Century Pillow-Talk: Applicability of the Marital Communications Privilege to Electronic Mail*, 58 S.C. L. REV. 275, 286 (2006) ("Most likely realizing the lack of Fourth Amendment protection afforded electronic communications, Congress enacted the Electronic Communications Privacy Act (ECPA) in 1986.").

29. 18 U.S.C. §§ 2510(15), 2711(2). An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). RCS "means the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). Electronic communications providers today (for example, e-mail providers) generally offer both of these services concurrently.

Whether a service provider is characterized as an ECS or a RCS greatly impacts what privacy rules protect the stored information.[30] For instance, the government must have a search warrant to access the contents of electronic communications stored with an ECS for less than 180 days.[31] Meanwhile, the government only needs a subpoena or court order (and no probable cause) to obtain the contents of electronic communications stored in a RCS, as long as it provides the subscriber with prior notice.[32]

Categorizing a cell phone provider as either an ECS or a RCS has presented difficulties in the lower courts. In at least one civil action involving the search of an employee's text messages, the issue of whether a service provider constituted an ECS or a RCS determined the employer's liability.[33] In 1986, Congress was concerned with the privacy of information stored on large, centralized servers.[34] This type of storage is vastly different from the type of storage performed by a SMC or cell phone provider. Accordingly, courts wrestle with this issue, and commentators believe the SCA is outdated.[35]

Additionally, the SCA is deficient in one key aspect—it offers no suppression remedy for criminal defendants.[36] In a motion to suppress, criminal defendants must seek protection for electronic communications under the Fourth Amendment.[37] Therefore, the SCA will appear only in civil actions involving the alleged unlawful search and seizure of text messages. Because this Note addresses what happens in a criminal motion to suppress, it is primarily concerned with applying existing Fourth Amendment doctrines rather than the SCA.[38]

30. Because current service providers can act both as ECS, RCS, or neither, depending on the circumstances, these categories have yielded confusing results in the courts. For example, in a recent Ninth Circuit case, the court reversed the part of the district court opinion finding that a text message provider was a RCS. *Quon*, 529 F.3d at 903. Under the SCA, an ECS has different disclosure duties, which in turn affected the outcome of the case. *Id.* at 901.

31. 18 U.S.C. § 2703(a).

32. *Id.* § 2703(b). The statute also authorizes the government to give a subscriber delayed notice in certain circumstances, thus temporarily avoiding the prior notice requirement. *Id.*

33. *Quon*, 529 F.3d at 903.

34. Kerr, *supra* note 28, at 1213.

35. *See, e.g.*, *Quon*, 529 F.3d at 903; Kerr, *supra* note 28, at 1208–09.

36. *See* Kerr, *supra* note 28, at 1241; Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, ¶ 4, http://www.lawtechjournal.com/articles/2007/02_070426_lawless.pdf. Despite this fact, at least one district court recently applied the SCA to a criminal case and determined that, because there was "no constitutional violation of the Stored Communications Act," "exclusion of the evidence [wa]s not available as a remedy." United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *2 (W.D. Ky. Aug. 17, 2009). This finding highlights the confusion in the lower courts—there can be neither a "constitutional violation" of a purely statutory right, nor an exclusionary remedy in the SCA.

37. As this Note is concerned with criminal liability, it largely focuses on the Fourth Amendment. If Congress chooses to amend the Stored Communications Act to include an exclusionary remedy, it would likely have a similar effect as the Wiretap Act had in regulating the use of wiretaps in criminal investigations.

38. Professor Kerr summarized why the Fourth Amendment offers insufficient protection for electronic communications, especially information transmitted over the Internet. Kerr, *supra* note 28, at 1209–12. First, the third-party doctrine defeats an individual's reasonable expectation of privacy in

C. The Fourth Amendment

Cases involving Fourth Amendment challenges to the search or seizure of text messages have thus far analogized text messages to both oral communications and to the contents of a closed container.[39] Although these analyses generally overlap and intertwine in the lower courts' opinions, the Note will discuss each in turn. First, this Section will discuss the Fourth Amendment as applied to spoken communications. As part of that discussion, the Note describes the *Katz* test and its relevance in determining whether an individual has standing to contest a search or seizure under the Fourth Amendment. Next, this Section addresses an important element of the *Katz* test and an exception to a defendant's ability to contest a search or seizure—the third-party doctrine. The Section then turns to the Fourth Amendment doctrines governing letters and written communications. Next, it discusses an alternative to the *Katz* test controlling workplace communications—the operational realities test. Lower courts have applied this test in determining whether employees have standing to contest the search and seizure of text messages sent via employer-owned cell phones and pagers.[40] Finally, this Section discusses *Kyllo v. United States*,[41] which demonstrates the Supreme Court's most recent approach to adapting the Fourth Amendment to technological advances.

1. The Fourth Amendment and Oral Communications

The seminal Supreme Court case addressing the intersection between communications and the Fourth Amendment is *Katz v. United States*.[42] In *Katz*, FBI agents placed a microphone-like "electronic listen-

electronic communications because one exposes private information to a third party (the service provider) simply by using the Internet. *Id.* at 1209–10. Second, the government could obtain information from third-party Internet and wireless service providers through a grand jury subpoena, which would not require probable cause. *Id.* at 1211. Third, service providers are private entities and, thus, can voluntarily disclose information to the government without even implicating the Fourth Amendment. *Id.* at 1212. As a result, Professor Kerr advocates for revising the SCA. *Id.* at 1208. Below, this Note discusses how commentators and judges have challenged whether the third-party doctrine should be applied to electronic communications at all. *See infra* Part III.C.2. For example, Justice Marshall stated in *Smith v. Maryland* that the third-party doctrine necessitates a *knowing* disclosure of information to a third party. 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). Yet, whether one knowingly transmits information to a third party while using the Internet requires a case-specific inquiry into the user's mental state.

39. *See, e.g.*, *Quon*, 529 F.3d at 904–05; United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993). The Supreme Court of Ohio recently opined that the closed container analogy is out of date given the vast amount of information stored on even modern standard phones, let alone smart phones. State v. Smith, No. 2008-1781, 2009 WL 4826991, at *4 (Ohio Dec. 15, 2009). The court did not offer its own analogy, however, stating that "cell phones defy easy categorization." *Id.* at *5.

40. *See Quon*, 529 F.3d at 903–08.

41. 533 U.S. 27 (2001).

42. 389 U.S. 347, 353 (1967) (reaffirming that the Fourth Amendment applies to "the recording of oral statements" and dismissing the notion that a "search" requires physical trespass of property); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383 (1974); Kerr, *supra* note 13, at 815 (calling *Katz* the "leading case in Fourth Amendment law").

ing and recording device on the outside" of a telephone booth while the defendant placed calls that implicated him in a gambling ring.[43] This tactic allowed the police to hear Katz's end of the conversation without physically intruding into the phone booth.[44] The lower courts rejected Katz's argument that this constituted an unconstitutional search, finding no Fourth Amendment violation because the FBI agents only placed the device on the outside of the booth without physically entering the interior space.[45] In making this decision, the lower courts followed the "trespass" doctrine of *Olmstead v. United States*.[46]

At the time the lower courts decided *Katz*, the Supreme Court's test in *Olmstead* determined what constituted a search under the Fourth Amendment.[47] The Court in *Olmstead* held that the use of wiretaps did not implicate the Fourth Amendment.[48] Under the "trespass" doctrine, a Fourth Amendment search necessarily entailed a search of material things,[49] and required a "physical intrus[ion] into 'a constitutionally protected area.'"[50] Following this doctrine, the lower courts in *Katz* reasoned that, even assuming a phone booth is a constitutionally protected area, any search of the phone booth must include an element of physical intrusion into the space.[51]

Katz established for the first time that the Fourth Amendment applies to communications one seeks to preserve as private.[52] By reversing the lower courts, the Supreme Court expressly overruled the "trespass" doctrine and previous case law concerning wiretapping.[53] It stated that "the Fourth Amendment protects people not places"[54] and found the FBI's use of technology to overhear Katz's private conversations constituted an unconstitutional, warrantless search.[55] The Court found that

43. *Katz*, 389 U.S. at 348.
44. *Id.*
45. *Id.* at 348–49.
46. 277 U.S. 438, 464 (1928).
47. *See Katz*, 389 U.S. at 352–53.
48. *Olmstead*, 277 U.S. at 466.
49. *Id.* at 464.
50. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(a), at 431; *cf. Olmstead*, 277 U.S. at 464 (stating that a search occurred when "[t]here was actual entrance into the private quarters of [a] defendant and the taking away of something tangible").
51. *Katz*, 389 U.S. at 348–49.
52. *Id.* at 351–52.
53. *Id.* at 353.
54. *Id.* at 351. Despite this oft-quoted statement in *Katz*, the Court's analysis and Justice Harlan's concurrence were both firmly rooted in a sense of place. *See id.* at 351–52 (emphasizing how Katz shut the door and entered the phone booth, thereby closing off his conversations from an "uninvited ear"); *id.* at 361 (Harlan, J., concurring) (stating that an individual's reasonable expectation of privacy "[g]enerally . . . requires reference to a 'place'" because "conversations in the open would not be protected against being overheard"). Professor Kerr believes that legal scholars are often too focused on the rhetoric of *Katz* and thus overstate the jurisprudential shift that actually occurred. Kerr, *supra* note 13, at 816. Accordingly, it would be more appropriate to view *Katz* as part of a shift in Fourth Amendment doctrine away from a strict analysis based on common law property rules toward a more nuanced analysis focusing on whether the individual has some control over the area or object in question. *Id.* at 818.
55. *Katz*, 389 U.S. at 351–52.

what one "seeks to preserve as private . . . may be constitutionally protected" so long as it is not "knowingly expose[d] to the public."[56] Thus, because Katz entered the booth with the intent to keep his conversation private and did not knowingly expose it to the public, he was entitled to Fourth Amendment protection.[57] The Court departed from its previous jurisprudence that did not protect communications alone and found that oral communications may fall under the purview of the Fourth Amendment.[58]

Justice Harlan's concurrence in *Katz* outlined a two-part test delineating what constitutes a search under the Fourth Amendment. The test states that the Fourth Amendment applies when (1) an individual has a subjective expectation of privacy and (2) society deems that expectation objectively reasonable.[59] After *Katz*, if a communication satisfies both prongs of Harlan's test, the individual who made it has standing for a Fourth Amendment claim as to that communication.[60]

2. An Exception to Standing: The Third-Party Doctrine

The third-party doctrine is one method by which a party can fail the *Katz* standing test. The Supreme Court stated in *Katz*, "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[61] The resulting doctrine states that one assumes the risk of exposure, and loses an expectation of privacy, in information knowingly revealed to a third party.[62] There is an implied assumption of

56. *Id.*

57. *Id.* at 353.

58. *Id.* at 351–52. Scholars dispute whether the majority opinion in *Katz* truly stands for the proposition that the Fourth Amendment protects the right to privacy in oral communications, especially absent an additional factor tying privacy to a place. *Compare* Kerr, *supra* note 13, at 822 (stating that Katz in effect temporarily rented out the phone booth, giving him a momentary property interest in that area, which in turn made his expectation of privacy reasonable), *with* Lawless, *supra* note 36, ¶ 8 (discussing that the Court, "at least rhetorically," shifted its Fourth Amendment concerns to notions of privacy rather than property), *and* David A. Sklansky, *Back to the Future:* Kyllo*,* Katz*, and the Common Law*, 72 MISS. L.J. 143, 147 (2002) (declaring that the "solution" to problems of modern-day surveillance measures is to "recogniz[e] that the Fourth Amendment protects communications as well as places" and "that virtual places as well as physical places can receive Fourth Amendment protection").

59. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Scholars criticize the *Katz* test for various reasons; for example, the "objective" prong of the test amounts to what the sitting Court thinks is reasonable at the time. Sklansky, *supra* note 58, at 157–58. This criticism, however, applies to any of the Court's objective tests. Other critics object to the subjective prong because one loses a subjective expectation of privacy if she believes she is being overheard, whether correctly or not. *See* Amsterdam, *supra* note 42, at 384. Professor LaFave writes that courts in practice do not give much credence to the subjective factor. 1 LAFAVE, *supra* note 50, § 2.1(c), at 438.

60. Rakas v. Illinois, 439 U.S. 128, 140 (1978) (articulating the *Katz* test in terms of whether one has "standing" to make a Fourth Amendment claim); s*ee also* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) (describing the threshold issue of a defendant's right to make a Fourth Amendment claim regarding a communication as whether the defendant had a reasonable expectation of privacy).

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

62. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third par-

the risk in conveying information to a third party so that it is no longer private. If applied literally, the third-party doctrine would eliminate a reasonable expectation of privacy in all electronic communications, including text messages, e-mail, and instant messages, because they inherently require exposure to a service provider's network.[63]

The Supreme Court has applied the third-party doctrine in the context of telephone communications before. In *Smith v. Maryland*, it found that a phone user has no legitimate expectation of privacy in phone numbers dialed because that information is knowingly exposed to a third party—namely, the phone company.[64] The Court analogized the telephone company's switching equipment to a live operator, finding that a phone user knowingly exposes the number to the telephone company via its switching equipment.[65] Therefore, an inanimate object takes the place of the third party in this context.[66] Justice Marshall dissented, finding the assumption of the risk analysis inappropriate where the phone user has no choice but to expose the information as a condition for using the technology.[67] He further stated that, even assuming individuals "knowingly" expose information to a third-party telephone company, "it does not follow that they expect this information to be made available to the public in general or the government in particular."[68]

When determining whether an individual has standing to contest the search and seizure of text messages, courts have not always applied the third-party doctrine.[69] If courts did apply the third-party doctrine, a user would never have a reasonable expectation of privacy in at least the numbers dialed because that information is always exposed to both the SMC and the service provider.[70] Instead, courts have applied the operational realities test or analyzed the issue solely in relation to the physical device carrying the messages.[71]

---

ties."); Lawless, *supra* note 36, ¶¶ 6, 9, 33 (explaining that the third-party doctrine, based on the idea that one assumes the risk of exposure by transmitting information to a third party, applies to electronic communications).

63. Courts, however, struggle to determine whether an individual has a reasonable expectation of privacy in electronic communications. For example, with e-mail courts have alternatively held that (1) users lose a legitimate expectation of privacy in the subscriber information only; (2) users have no expectation of privacy at all once the e-mail is delivered to its recipient (analogizing the e-mail to a letter received); or (3) users have no legitimate expectation in the to/from and subject lines, but a user does have a legitimate expectation in the contents of the e-mail (analogizing the to/from and subject lines to "envelope" information in a letter). *See, e.g.*, Lawless, *supra* note 36, ¶¶ 17, 22–24; Story, *supra* note 28, at 285–86.

64. *Smith*, 442 U.S. at 743–44.

65. *Id.* at 744 ("The switching equipment . . . is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.").

66. *See id.*

67. *Id.* at 749–50 (Marshall, J., dissenting) (finding it "idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative").

68. *Id.* at 749.

69. *See infra* Part III.C.

70. *See supra* notes 19–21 and accompanying text.

71. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 907 (9th Cir. 2008).

3. Letters and Written Communications

In Fourth Amendment jurisprudence, letters and written communications are not entirely analogous to oral communications. For purposes of determining if one has a reasonable expectation of privacy in a letter, courts make two distinctions: (1) between "envelope" information and "content" information, and (2) between a letter in transit and a letter received.[72] The content/envelope distinction is an exception to the third-party doctrine that shields information an individual takes extra steps to keep secret (the contents of the envelope) and applies the doctrine only to what is exposed—namely, the envelope information.[73] In *Smith v. Maryland*, one reason the Court concluded that pen registers do not violate an individual's reasonable expectation of privacy is because it analogized the phone numbers to "envelope" information and the conversation to "content" information.[74]

Courts also distinguish between a letter received and a letter in transit.[75] While in transit, the content/envelope distinction applies because at that point the sender knowingly exposes only the envelope information.[76] Once the recipient has possession of the letter, however, the sender loses an expectation of privacy in the contents as well because the recipient can reveal its contents to others.[77] If the sender retains a copy, the retained copy is part of her personal effects and is protected accordingly.[78]

In the context of text messages, analogizing to letters has at least two potential consequences. First, courts could conclude that senders have no reasonable expectation of privacy in the recipient information (i.e., the phone number or numbers) when the message is transmitted. Second, once the message is successfully transmitted to the recipient's device, the sender would lose a reasonable expectation of privacy in the entire message.

72. *See Ex parte* Jackson, 96 U.S. 727, 733, 735 (1878); Lawless, *supra* note 36, ¶ 16

73. Lawless, *supra* note 36, ¶ 16.

74. *See* Smith v. Maryland, 442 U.S. 735, 741 (1978) ("[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

75. *Ex parte Jackson*, 96 U.S. at 733, 735.

76. *See* Kerr, *supra* note 28, at 1228 (distinguishing "envelope" information from the content of communications).

77. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

78. This dichotomy is analogous to the problem with sent text messages. Courts have found that a defendant has a legitimate expectation of privacy in the messages stored on her own phone, regardless of whether they are sent or received, but not in messages sent to another person and stored on the recipient's phone. *See infra* Part III.C.

4. The "Operational Realities" Test and Workplace Communications—An Alternative Privacy Inquiry

In addition to the *Katz* test, courts have applied the operational realities test to determine if one has Fourth Amendment standing to contest cell phone searches in the context of employment.[79] Under the operational realities test, an employee has a reasonable expectation of privacy in an area (or a communication) if her employer's day-to-day operations indicate that expectation is reasonable.[80] This is an extremely case-sensitive analysis.[81] For example, in *O'Connor v. Ortega*, the Supreme Court determined that a hospital employee had a reasonable expectation of privacy in his desk and file cabinets because, among other things, he had a private office that he had occupied for the previous seventeen years and he habitually kept personal items there.[82]

While not technically an exception to the third-party doctrine, this analysis has the effect of enhancing an employee's expectation of privacy in electronic communications if (1) the employer has a property interest in the device or controls the network, and (2) the employer has a policy, written or understood, of not reading those communications.[83] In a recent Ninth Circuit decision, the court determined that a sheriff's department employee had standing to contest the search of text messages sent via department-issued pagers.[84] According to the department's informal policy, supervisors would not audit messages so long as employees paid overage fees.[85] The department's own informal policy created the employee's reasonable expectation and subsequent standing to contest the search.[86]

5. The Fourth Amendment in the Face of Technological Advances

The Supreme Court has discussed how technological advances may affect an individual's reasonable expectation of privacy under the *Katz* test. In 2001, the Court decided *Kyllo v. United States*, which determined whether an individual had a reasonable expectation of privacy to chal-

79. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 907 (9th Cir. 2008) (finding dispositive the employer's unwritten policy of not auditing the content of employees' text messages).

80. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) ("[T]he operational realities of the workplace . . . make *some* employees' expectations of privacy unreasonable" and make others reasonable).

81. *See id.* at 718.

82. *Id.* at 718–19.

83. *See Quon*, 529 F.3d at 907.

84. *Id.* at 904.

85. *Id.* at 897.

86. *Id.* at 906. *Quon* is the most recent and prominent case regarding an individual's ability to challenge the search or seizure of text messages. Because the court used the operational realities test, it is an open question whether and how the *Katz* test applies to text messages. The Supreme Court has granted certiorari and may decide the case on a broader issue; namely, whether senders of text messages have a reasonable expectation of privacy under the *Katz* test. Certiorari was granted under the name *City of Ontario, California v. Quon*, No. 08-1332, 2009 WL 1146443, at *1 (U.S. Dec. 14, 2009).

lenge the use of a thermal imaging device.[87] Government agents, suspecting the defendant was growing marijuana plants, aimed the device at the defendant's home to detect excess heat emitted by high-intensity lamps used to grow the plants.[88] Justice Scalia, writing for a five-justice majority, framed the issue in the following way: to determine "what limits there are upon th[e] power of technology to shrink the realm of guaranteed privacy."[89] The majority held that the use of the thermal imaging device constituted a Fourth Amendment search, basing its decision on two factors: (1) thermal imaging devices are "not in general public use," and (2) the information garnered regarding the inside of the defendant's home would have been otherwise "unknowable without physical intrusion."[90]

Given the decision in *Kyllo*, scholars dispute whether courts should grant greater privacy protections in the face of new technological advances or whether Justice Scalia's focus on the home as a locus of special protection actually indicates a withdrawal from the privacy protections promised in *Katz*.[91] The Court is concerned with the potential for police to use technology to expose extremely private information, but it frames the discussion in terms of protecting the "intimate details" associated with the home.[92]

The circumstances in *Kyllo* are distinguishable from the search and seizure of text messages. First, electronic communications are part of a network that is not, by its nature, grounded in a place. The *Kyllo* Court specifically linked its holding with the place of the intrusion—the home.[93] Second, the *Kyllo* Court addressed the issue of whether the police may use technology to assist their investigations.[94] It is still an open question whether *Kyllo* restricts or enhances protections for private individuals' use of technology.

D. The Fourth Amendment and Containers

Another determinative issue in the lower courts' application of the Fourth Amendment to text messages is whether, and under what cir-

87. 533 U.S. 27, 29 (2001).

88. *Id.* at 29.

89. *Id.* at 34.

90. *Id.* at 40.

91. *Compare* Kerr, *supra* note 13, at 832 ("Although these cases (and particularly *Kyllo*) can be read plausibly as suggesting a broad and even creative view of how the Fourth Amendment should respond when technology threatens privacy, I think a better reading is that these cases are essentially conservative, reinforcing the primacy of property law."), *with* Sklansky, *supra* note 58, at 188, 210 (stating that "*Kyllo* is less important for its result than for its jurisprudence" and suggesting that *Kyllo* is "promising" because it potentially combats the ability of technology to erode privacy).

92. *Kyllo*, 533 U.S. at 38.

93. *Id.* at 35–36 (describing a desire to avoid "leav[ing] the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home").

94. *See id.* at 33–40.

cumstances, police may lawfully search a container without a warrant.[95] In *New York v. Belton*, the Court defined a "container" as "any object capable of holding another object," and said that it included "receptacles."[96] Several courts have analogized cell phones to containers, although the comparison is at least challengeable given that electronic data are not technically "objects."[97] The Court has developed several bright-line rules dealing with containers with the primary goal of guiding police officers in the field.[98] In the Court's most recent Fourth Amendment decision, *Arizona v. Gant*, it initiated a withdrawal from the bright-line approach in favor of an approach in accord with the doctrines' underlying rationales.[99]

Under the search incident to arrest doctrine, police often have authority to search containers without a warrant. The doctrine began with the Court's 1969 *Chimel v. California* decision.[100] In *Chimel*, the Court held that police have authority to search the area in the arrestee's immediate control incident to a lawful arrest.[101] Two governing rationales justified the doctrine: (1) ensuring police safety, and (2) preventing the destruction of evidence.[102] Four years later, the Court extended the search incident to arrest doctrine, authorizing police to search all containers found on an arrestee's person.[103] The Court reasoned against a case-by-case analysis and in favor of a clear, bright-line rule that did not require on-the-spot police interpretation.[104]

Home arrests can present distinct issues pertaining to container searches. Two doctrines intersect when arrests occur at home—the search incident to arrest doctrine and the plain view doctrine. The police may still conduct a search incident to arrest of the person and containers in the area of the arrestee's immediate control.[105] Items not within the arrestee's immediate control present a different issue. Under the "plain view" doctrine articulated in *Arizona v. Hicks*, the police can seize an

95. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 580 (1991) (containers "incidentally" in a car); United States v. Chadwick, 433 U.S. 1, 15 (1977) (containers on a person).

96. 453 U.S. 454, 460–61 n.4 (1981).

97. *See* State v. Smith, No. 2008-1781, 2009 WL 4826991, at *4 (Ohio Dec. 15, 2009).

98. *See Belton*, 453 U.S. at 458 (favoring bright-line rules that allow police to "reach a correct determination beforehand as to whether an invasion of privacy is justified," avoiding on-the-spot deliberation and interpretation (quoting Wayne R. LaFave, *"Case-By-Case Adjudication" Versus "Standardized Procedures": The* Robinson *Dilemma*, 1974 S. CT. REV. 127, 142)).

99. Arizona v. Gant, 129 S. Ct. 1710, 1719 (2009).

100. 395 U.S. 752 (1969); *see also* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. Rev. 27, 33 (2008) (calling *Chimel* the "doctrine's modern conception").

101. *Chimel*, 395 U.S. at 763.

102. *Id.*

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

104. *Id.* at 235 ("A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick *ad hoc* judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search."). This arguably obliterates the first rationale of officer safety, but is supported as a means of alleviating an officer's need for discretion in borderline cases.

105. *Chimel*, 395 U.S. at 763.

item in plain view when (1) the police are lawfully in a place (for example, pursuant to an arrest or search warrant), (2) they a have a right to access the area where they found the item, and (3) the incriminating nature of the item is immediately apparent (i.e., the police have probable cause to believe the item is contraband).[106]

Vehicles present a somewhat more complicated issue with the search incident to arrest doctrine. Before the Court's April 2009 decision in *Gant*, the police had broad (and somewhat troubling) discretion to search vehicles incident to a lawful arrest.[107] In *New York v. Belton*, the Court authorized a search of the entire passenger compartment of a car, and all containers found therein, incident to a lawful arrest (i.e., an arrest based on probable cause, but not necessarily a warrant).[108] In 2004, the Court extended this bright-line rule to include cars that an arrestee recently occupied.[109] *Gant* restricts these two prior holdings.[110] Justice Stevens' majority opinion rejected a broad reading of *Belton* that allowed for "a vehicle search incident to the arrest of a recent occupant even if there is no possibility the arrestee could gain access to the vehicle at the time of the search."[111] Instead, the Court articulated its vehicular search incident to arrest doctrine anew, claiming to be more in line with the dual rationales of *Chimel*.[112] The search of a "vehicle incident to a recent occupant's arrest [is authorized] only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search."[113] A vehicle search is also authorized when an officer reasonably determines that evidence of a crime is within the vehicle.[114]

The State of Arizona advocated for the broad—and then widely accepted—reading of *Belton*; namely, that officers may search the passenger compartment of a vehicle and all containers within incident to any

106. 480 U.S. 321, 326–27 (1987) ("[P]robable cause is required in order to invoke the 'plain view' doctrine . . . . To say otherwise would be to cut the 'plain view' doctrine loose from its theoretical and practical moorings. The theory of that doctrine consists of extending to nonpublic places such as the home, where searches and seizures without a warrant are presumptively unreasonable, the police's longstanding authority to make warrantless seizures in public places of such objects as weapons and contraband.").

107. *See* WAYNE R. LAFAVE ET AL., PRINCIPLES OF CRIMINAL PROCEDURE: INVESTIGATION 153 (2004) ("[T]he results produced under the *Belton* 'bright-line' well exceed those that usually would be reached . . . [under] *Chimel*. This is particularly troubling when it is considered that *Belton* permits broad searches of vehicles without any probable cause that evidence will be found therein, provided only that there is probable cause to arrest an occupant.").

108. 453 U.S. 454, 460 (1981).

109. Thornton v. United States, 541 U.S. 615, 623–24 (2004).

110. Arizona v. Gant, 129 S. Ct. 1710, 1719 (2009).

111. *Id.* at 1718. Justice Scalia joined the majority opinion to avoid a 4-1-4 split, but thought "this standard fails to provide the needed guidance to arresting officers." *Id.* at 1724 (Scalia, J., concurring). Justice Scalia prefers to "simply abandon the *Belton-Thornton* charade of officer safety" and "hold that a vehicle search incident to arrest is *ipso facto* 'reasonable' only when the object of the search is evidence of the crime for which the arrest was made, or of another crime that the officer has probable cause to believe occurred." *Id.* at 1725 (Scalia, J., concurring).

112. *Id.* at 1719.

113. *Id.*

114. *Id.*

lawful arrest.[115] The State argued this bright-rule marked the appropriate balance between law enforcement interests and privacy interests.[116] Justice Stevens opined that "the State seriously undervalues the privacy interests at stake," ignoring the "central concern" of Fourth Amendment jurisprudence—prohibiting officers from "rummag[ing] at will among a person's private effects."[117] This marks a departure from the Court's previous adherence to bright-line rules and creates a potential opening for protecting the privacy of all contents of a cell phone, including text messages, unless an officer has a warrant or probable cause to believe the phone contains evidence of a particular crime.

When not incident to a lawful arrest, searches of containers located in a car present a different issue. Police can search containers in vehicles not incident to arrest with either (1) probable cause to search the container[118] or (2) probable cause to search the car for an item (if that the item could feasibly be found inside the container searched).[119]

If police conduct a stop-and-frisk pursuant to *Terry v. Ohio*, container searches are only authorized if the container could hold a weapon.[120] This is because unlike a search incident to arrest that is justified on the dual bases of officer safety and preservation of evidence, officer safety is the sole justification for a *Terry* stop.[121] If an officer perceives that the container could not contain a weapon, the officer's safety is not at risk and a search is impermissible.[122] Cell phones therefore would not be searchable pursuant to a *Terry* stop.

Exigent circumstances may also apply to container searches. In situations where an individual has a container—but is not arrested, not frisked, and not in a car—the Court's holding in *United States v. Chadwick* is still good law.[123] In *Chadwick*, the Court stated that probable cause and a warrant are required to search the contents of a container unless the search is pursuant to an arrest or some other exigent circumstances exist.[124] Once the police gain control over the container and the container is no longer within the arrestee's immediate control, *Chadwick*

115. *Id.* at 1718, 1720.

116. *Id.* at 1720.

117. *Id.*

118. California v. Acevedo, 500 U.S. 565, 573 (1991) (requiring only probable cause as to the contents to search a container found in a car).

119. *Id.* at 580 ("The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained.").

120. Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) (disallowing the search of a pocket when "the officer already knew [it] contained no weapon").

121. Terry v. Ohio, 392 U.S. 1, 27 (1968) (describing a "narrowly drawn authority" to search for weapons and ensure officer safety).

122. *See id.*

123. The rule espoused in *Chadwick*, that the Warrant Clause applies to containers regardless of whether they are found in a vehicle, was abrogated by *Belton*. The abrogation should be reexamined in light of *Gant*.

124. United States v. Chadwick, 433 U.S. 1, 11 (1977) (holding that, where there is no exigency, it is unreasonable for the Government to search a container without a warrant).

applies and the police need a warrant to examine its contents.[125] On the other hand, if law enforcement officers have reason to believe the search is imminently necessary, then a warrant may not be required.[126]

Therefore, there are at a minimum five distinct situations that deal with warrantless container searches: (1) searches incident to arrest, (2) vehicle searches incident to arrest, (3) searches of containers in cars where probable cause exists, (4) searches pursuant to a *Terry* stop, and (5) searches of containers under exigent circumstances. These doctrines are all relevant to the search and seizure of text messages if a court analogizes a cell phone to a container.

This Part has outlined the relevant background information on text message technology, the Stored Communications Act, and Fourth Amendment search and seizure doctrine. The following Part elaborates on these concepts, analyzing how courts and scholars have applied them in the context of text messages.

III. ANALYSIS

Lower courts have used various analogies to apply Fourth Amendment doctrines to both text messages and cell phone technology generally. Partly because of the immense amount of personal data that is stored in recent generations of cell phones, the current analyses are insufficient. The SCA could be an alternative, much as the federal Wiretap Act has codified the use of wiretaps during investigations.[127] That Act, however, is demonstrably insufficient as it currently stands. This Part briefly discusses how the SCA lacks proper protections for criminal defendants and then discusses the analogies courts and scholars have used in adapting Fourth Amendment jurisprudence to cell phone technology.

A. The Insufficiency of the Stored Communications Act

When Congress enacted the SCA in the mid-1980s, it recognized that the Fourth Amendment would not protect electronic communications, despite a user's reasonable expectation that those communications remain private.[128] The SCA regulates when a private service provider can disclose its customers' information.[129] As the Act does not contain an exclusionary remedy, Congress did not appear overly concerned about the use of electronic communications in criminal prosecutions.[130] Criminal

125. *Id.* at 15. This is true as long as some other exigency does not exist at the time. *Id.* at 15 n.9.

126. *See id.* at 14.

127. LAFAVE ET AL., *supra* note 107, § 3.6, at 248.

128. *See* Kerr, *supra* note 28, at 1209, 1213 ("To understand the SCA, it helps to begin by considering why Congress enacted the statute in the first place. . . . Although the private search doctrine of the Fourth Amendment allows private providers to [disclose information], the SCA imposes limitations on the circumstances in which such a disclosure can occur.").

129. *Id.* at 1213.

130. *Id.* at 1241.

defendants must rely on the Fourth Amendment. This is ironic considering the SCA was enacted specifically to address the Fourth Amendment's insufficiencies.[131]

Several commentators have recommended that Congress rectify the SCA's deficiency relating to criminal prosecutions by amending the SCA.[132] Professor Gershowitz has suggested legislators are more likely to create greater protections in this area.[133] Because text messages and other information stored in cell phones can become evidence in white collar prosecutions and middle-class legislators can relate to white collar defendants, legislators may be less likely to take a tough-on-crime stance.[134] While other parts of the ECPA, including the Wiretap Act, contain a suppression remedy,[135] criminal defendants remain in legal limbo with regards to their text and pix messages. To understand how courts address the search and seizure of text messages, therefore, it is necessary to turn to the Fourth Amendment.

B. Whether Defendants Have Standing Under the Fourth Amendment

To implicate the Fourth Amendment, an individual must have a reasonable expectation of privacy in the text messages searched or seized.[136] Courts have used two tests to find that individuals have a reasonable expectation of privacy in text messages.[137] This Section first addresses the *Katz* test and then turns to the operational realities test, assessing when each test may apply to text messages.

1. Reasonable Expectation of Privacy Under the Katz *Test*

In *Rakas v. Illinois*, the Supreme Court stated that standing under the Fourth Amendment is virtually equivalent to the *Katz* test.[138] Therefore, if a defendant has a reasonable expectation of privacy in a cell

131. *Id.* at 1209–13.

132. *See, e.g.*, Gershowitz, *supra* note 100, at 50 (suggesting that state legislatures create more stringent protections); Kerr, *supra* note 28, at 1233 (recommending "four potential areas of reform for the SCA").

133. Gershowitz, *supra* note 100, at 52–53.

134. *Id.* (suggesting that middle-class legislators will be more likely to increase statutory protections for text messages and other electronic communications, even through legislation that may not be "anti-crime," because they are more likely to know someone affected by these searches or be affected themselves).

135. *See* LAFAVE ET AL., *supra* note 107, § 3.6, at 248 (stating that the Wiretap Act "at one point declares that no information derived from eavesdropping 'may be received in evidence in any trial, hearing, or other proceeding'" if seized in violation of the Act); Morgan, *supra* note 27, at 815 ("Suppression of evidence obtained in violation of the ECPA is available for wire or oral communications, but is inexplicably absent for e-mail.").

136. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008).

137. *See, e.g.*, *id.* at 903–07 (applying operational realities test); United States v. Finley, 477 F.3d 250, 258 (5th Cir. 2007) (applying the *Katz* test).

138. Rakas v. Illinois, 439 U.S. 128, 143 (1978) ("[T]he Court in *Katz* held that capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.").

phone and its contents, she has standing to contest the search or seizure of the phone's contents, including text messages.[139] When a defendant sends messages to another person there are additional issues, requiring the courts to assess whether the defendant maintains a reasonable expectation of privacy in those sent messages.

Several lower courts have held that individuals have a reasonable expectation of privacy in text messages.[140] Those courts distinguish between the phone as a possession (a container) and the actual transmission of information (a communication).[141] If the phone is analogous to a container, the owner or possessor of the phone has a reasonable expectation of privacy in the contents (the messages) just as the owner or possessor of, for example, an address book.[142]

In contrast, if an individual sends a text message and then claims Fourth Amendment standing as to that message existing somewhere other than the sender's own phone, the third-party doctrine easily defeats the sender's claim.[143] Under the assumption of the risk analysis espoused in *Katz*, the knowing revelation of information to another party defeats a reasonable expectation of privacy in communications, including electronic communications.[144] For example, one federal district court found that the third-party doctrine defeated a defendant's reasonable expectation of privacy in his Internet Service Provider's (ISP) records because he "knowingly" revealed that information to the ISP.[145]

Applying the third-party doctrine, a user would not have a reasonable expectation of privacy under the *Katz* test as to the messages not

139. *See, e.g.*, *Quon*, 529 F.3d at 904 (stating that the "threshold question" of standing is determined by whether users "have a reasonable expectation of privacy in their text messages"); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (finding that the defendant had standing to contest the search of a pager's contents because he "maintained a subjective expectation that . . . [it] would be free from governmental invasion" and that expectation was objectively reasonable).

140. *See Quon*, 529 F.3d at 905; *Finley*, 477 F.3d at 259. *But see* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("So long as the risk-analysis approach of *Katz* [(i.e., the third-party doctrine)] remains valid, . . . this court is compelled to apply traditional legal principles . . . [and] deny Mr. Hambrick's motion to suppress.").

141. *See Finley*, 477 F.3d at 259 (finding a reasonable expectation of privacy in text messages as contents of a container—the cell phone); *Chan*, 830 F. Supp. at 534 (stating that the transmitter of a message would not have the same expectation of privacy as the possessor of a pager because the transmitter releases the information to the person on the receiving end to do with it as he or she wishes).

142. *See Finley*, 477 F.3d at 259; *Chan*, 830 F. Supp. at 534; State v. Novicky, No. A07-0170, 2008 WL 1747805, at *4 (Minn. Ct. App. Apr. 15, 2008). The following Section discusses the container analogy in depth.

143. *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) (analogizing a received e-mail to a received letter and concluding that the sender lacks a reasonable expectation of privacy); United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005) (finding no reasonable expectation of privacy to prevent recipient from disclosing contents of text message); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (finding no expectation of privacy in e-mail once received); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (defeating a claim as to e-mail once recipient receives message).

144. *Cf. Hambrick*, 55 F. Supp. 2d at 508 (stating that the court "is compelled to apply" the *Katz* risk analysis to new technologies when a user discloses information to third parties, thereby defeating any reasonable expectation of privacy under "traditional legal principles").

145. *Id.* at 505, 508.

stored in the user's own mobile device. Text messages can exist in various places besides a sender's phone; for example, in a SMC,[146] in the recipient's phone, or as part of the service provider's temporary or permanent records.[147] If a court finds that a sender knowingly reveals information to any of these parties, the sender has no legitimate expectation of privacy under the *Katz* risk analysis.[148] At a minimum, the sender has no reasonable expectation of privacy permitting a challenge to the search of messages on a recipient's phone because the sender knowingly reveals the information to the recipient.[149]

The search and seizure of information from a SMC or the defendant's service provider presents distinct and more difficult issues, but the same result is likely—at least regarding the recipient's phone number.[150] In those instances, the content/envelope distinction could prevent access to the contents of a text message. Following the rationale of *Smith v. Maryland*, the sender knowingly reveals the recipient's phone or pager number to the SMC because the revelation is necessary to ensure transmittal.[151]

When a service provider retains records, however, a user's reasonable expectation of privacy would depend on the nature of the retention and its duration. For instance, some service providers retain records of the actual message content for an extended period of time.[152] Because service providers are private third parties, they can voluntarily disclose these records to the police, subject to restrictions under the SCA.[153] The

146. Gupta, *supra* note 17.

147. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 896 (9th Cir. 2008) (stating that text messages in one instance were archived after being stored on the system server for 72 hours).

148. Justice Marshall's dissent in *Smith v. Maryland* questioned whether one can be said to "knowingly" disclose any information at all absent individual choice. 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). In discussing whether a telephone user knowingly discloses the phone number dialed to the phone company, the majority stated that, regardless of whether the dialer has any subjective expectation of privacy in the number dialed, that expectation is not legitimate. *Id.* at 745 (majority opinion). The majority's rationale is that "users realize that they must 'convey' phone numbers to the telephone company" in order to reach the party on the other line. *Id.* at 742. Justice Marshall countered that, even accepting this supposition, it does not follow that one loses an expectation of privacy in the information: "[E]ven assuming, as I do not, that individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular." *Id.* at 749 (Marshall, J., dissenting) (citations omitted).

149. *See* United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005) (determining that a recipient of a text message is like the recipient of any other communication and that the sender cannot expect to prevent the recipient's divulgence of information).

150. *See Smith*, 442 U.S. at 743–44 (finding no legitimate expectation of privacy in phone numbers, even if there is a reasonable expectation of privacy in the contents of a communication).

151. *See supra* notes 17–25 and accompanying text.

152. *See Quon*, 529 F.3d at 895–96; Flagg v. City of Detroit, 252 F.R.D. 346, 347–48 (E.D. Mich. 2008).

153. *See Quon*, 529 F.3d at 900 (explaining that "the SCA prevents 'providers' . . . from divulging private communications to certain entities and/or individuals" and the amount of protection depends on whether the provider is considered a RCS or ECS). The contents of text messages stored in a service provider's records, however, can be accessed by means of a grand jury subpoena or court order, both requiring less than probable cause. The Pen Register Act would likely apply as to the numbers

user would be permitted to make a Fourth Amendment challenge to the search only insofar as the user did not knowingly expose the message to the provider, which depends on the provider's disclosed message retention policies.

Courts also analogize sent text messages (and e-mails) to letters.[154] This analogy defeats a Fourth Amendment standing claim for two primary reasons: (1) the third-party doctrine,[155] and (2) the rule regarding letters received.[156] These doctrines are closely intertwined and generally reflect the application of the Court's Fourth Amendment risk analysis. If one voluntarily discloses information to a third party, that individual may disclose the information to others, including law enforcement officers.[157] Applying this analysis, the Eleventh Circuit held that a defendant had no standing to challenge a recipient from testifying at trial regarding the content of text messages.[158] Therefore, the third-party doctrine often presents difficulties in establishing standing to challenge the search and seizure of text messages under the *Katz* test.

2. The Operational Realities Test Applied to Text Messages

The irony of the operational realities test as applied to text messages is that employees transmitting text messages on an employer-owned pager or cell phone may have a reasonable expectation of privacy whereas individuals using their own phones would not. The third-party doctrine can diminish or defeat a reasonable expectation of privacy in a transmitted text message.[159] The operational realities of a workplace, however, can establish a reasonable expectation of privacy in text messages transmitted on an employer-owned phone or pager.[160]

The Ninth Circuit recently recognized an employee's reasonable expectation of privacy in text messages because the "operational reality" at the police department where he worked allowed personal text messag-

dialed, as when an individual dials a number to have a conversation. *See* 18 U.S.C. §§ 3121–3127 (2006).

154. *See Quon*, 529 F.3d at 906–07 (text message); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (e-mail); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (e-mail).

155. *Cf.* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) (stating that defendant has no reasonable expectation of privacy in subscriber information given to his Internet Service Provider because the voluntary turning over of information to third parties extinguishes that expectation).

156. *See, e.g.*, *Quon*, 529 F.3d at 906 (explaining that the sender of a text message has no reasonable expectation as to the recipient's actions).

157. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

158. United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005). The court determined that a sender has no reasonable expectation of privacy—and thus no standing to challenge—the recipient's testimony, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* (internal quotation marks omitted) (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

159. *See supra* Part II.C.2.

160. *See Quon*, 529 F.3d at 907.

es as long as the employee paid for overages.[161] The court held that, despite a written policy stating that a supervisor had a right to audit text message records, the employee had a reasonable expectation of privacy because it was the "informal policy" of the department that the supervisor would not do so.[162] Courts have applied the operational realities test to other forms of electronic communications as well.[163] The irony that state employees, utilizing their employer's pagers or cell phones, have a potentially greater privacy interest in text messages than individuals using their own phones demonstrates that the tests are inadequate as applied to text messages.

C. How the Government Can Seize Text Messages Stored in Phones

Typically, criminal prosecutions involving text messages result from the police seizing a suspect's phone and subsequently searching its contents.[164] Whether a search or seizure of text messages stored on cellular telephones is justified often turns on how one analogizes text messages. In large part, courts and scholars have used three analogies; they have compared text messages to letters, the contents of a container, and spoken communications. This Note addresses each of these analogies in turn.

1. The Letter Analogy

Some courts have analogized text messages discovered in cell phones and pagers to letters.[165] Following this analogy, senders have a reasonable expectation of privacy in the contents of the messages, but

161. *Id.*

162. *Id.*

163. *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) (files on a university computer server).

164. Therefore, while discovering vast amounts of incriminating evidence in a service provider's archives, as happened in the case of former Detroit Mayor Kwame Kilpatrick, may make for compelling public drama, it is more urgent to resolve the issues dealing with text messages found during the search of a suspect's phone. Service providers often keep records of sent text messages. *See Quon*, 529 F.3d at 895–96; Flagg v. City of Detroit, 252 F.R.D. 346, 347–48 (E.D. Mich. 2008). Although messages are generally stored on a wireless provider's server for a brief period, some providers will keep archived records indefinitely. These records can be obtained pursuant to the SCA with a grand jury subpoena or court order. *See supra* text accompanying notes 31–32. In August 2008, the Eastern District of Michigan also allowed civil discovery of text message records pursuant to Rule 26 of the Federal Rules of Civil Procedure. *Flagg*, 252 F.R.D. at 352. The district judge affirmed a magistrate judge's order to compel discovery of text messages pursuant to Rule 26 although the SCA does not contain any express language that allows for such discovery. *Id.* Review of these text messages led to charges against Kwame Kilpatrick and his Chief of Staff, Christine Beatty, for perjury and obstruction of justice. Kilpatrick pled guilty to the obstruction of justice charges. Jim Schaeffer et al., *supra* note 6.

165. This analogy has been used to a greater extent to describe e-mail and other communications stored on computers. As cell phones become more akin to handheld computers and cell phones are used just as often to send e-mails as text messages, this analogy may be used more readily to describe communications between cellular phones. *See, e.g.*, Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165, 1171–72 (2008).

not in the phone numbers associated with them.[166] Additionally, with the third-party doctrine, senders may not have a reasonable expectation of privacy with respect to text messages once received by or exposed to another person.[167]

Given the realities of modern technology, the letter analogy is insufficient and logically inconsistent. First, at the current rate, text messages are sent with much greater frequency than letters.[168] Second, text messages are transmitted virtually instantaneously.[169] Third, text messages can be stored on servers for unknown periods of time.[170] Fourth, while it is a federal offense for anyone but the recipient to open snail mail, there exists no similar protection for text messages.[171]

The fact that text messages are currently sent much more often than letters might not appear troublesome at first because the frequency should not affect the underlying rationale. Yet, while people send increasingly more text messages, doing so becomes habitual and, consequently, individuals take less care in the information they disclose. The case law demonstrates numerous instances of individuals planning drug deals or describing sexual escapades in text messages, demonstrating this lack of care.[172] While the Fourth Amendment is not intended to protect individuals from their own mistakes, it *is* intended to balance privacy interests with criminal law enforcement interests.[173] The Fourth Amendment protects both the innocent and the guilty,[174] making it imperative that one's privacy interest in a text message is not lost by its mere transmission. Otherwise virtually all text messages would be subject to search.[175] Although courts could still distinguish between sent and received messages, such a distinction would be incredibly difficult for po-

166. *See Quon*, 529 F.3d at 905.

167. *See id.* at 906; United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005).

168. *See* U.S. POSTAL SERV., POSTAL FACTS 2009, at 1 (2009), http://www.usps.com/communications/newsroom/facts/postalfacts2009.pdf (stating that the U.S. Postal Service delivered 203 billion pieces of mail in 2008); Nielson Wire, In U.S., SMS Text Messaging Tops Mobile Phone Calling (Sept. 22, 2008), http://blog.nielsen.com/nielsenwire/online_mobile/in-us-text-messaging-tops-mobile-phone-calling (stating that the average mobile phone customer sends 357 text messages per month, for a total of approximately 4284 per year). There are approximately 270 million cell phone users in the United States, for a total of 1157 trillion text messages per year. *See* Int'l Telecomm. Union, ICS Statistics Database, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx (follow "3. Mobile cellular, subscribers per 100 people" hyperlink) (last visited Jan. 28, 2010).

169. *See supra* Part II.A.

170. *See supra* notes 24–25 and accompanying text.

171. *See* 18 U.S.C. § 1708 (2006).

172. *See, e.g.*, *Quon*, 529 F.3d at 898 (sexually explicit messages); United States v. Finley, 477 F.3d 250, 254–55 & n.2 (5th Cir. 2007) (drug deals). The term "sexting" has even become a popular culture phenomenon after the Tiger Woods scandal. A Google search on January 25, 2010, returned 1,710,000 results for "Tiger Woods sexting."

173. *See* Arizona v. Gant, 129 S. Ct. 1710, 1720 (2009); Terry v. Ohio, 392 U.S. 1, 26–27 (1968) (balancing the interest in officer safety with the privacy interests of the suspect).

174. *See Terry*, 392 U.S. at 8–16 (discussing the need to balance individual privacy rights with the ability of police to function effectively).

175. *Cf.* Kerr, *supra* note 28, at 1210–11 (stating that the third-party doctrine potentially destroys any reasonable expectation of privacy in e-mails).

lice officers to apply in the field.[176] Therefore, if the third-party doctrine applies to text messages as it does to letters, law enforcement officers could access text messages without any level of suspicion because such an action would not implicate the Fourth Amendment.[177]

The letter analogy presents another problem due to the speed with which text messages are delivered. Text messages are sent—first via the service provider's network and then to the recipient's phone—in a few seconds, compared with letters, which take at least overnight to deliver.[178] Applying both the third-party doctrine and a letter analogy, any reasonable expectation of privacy that existed is obliterated just as quickly as the message is delivered.[179] This result may explain why courts more often treat text messages as the contents of a container.

Third, because of the varying periods of time text messages remain on a provider's network server, or in its archived records, it is unlikely that a user knows to what extent her text messages are actually exposed to third parties.[180] The assumption of the risk analysis, inherent in the third-party doctrine, logically necessitates some knowing exposure of information to another party.[181] While one does knowingly expose a text message to the recipient, it is unlikely that individuals understand precisely how text messages are transmitted.[182] This possibly explains why the Fifth Circuit did not address the third-party doctrine at all in determining that individuals have a reasonable expectation of privacy in text messages.[183] Fourth Amendment privacy concerns would be compromised by events out of the sender's control and circumstances that are likely unknown. Although this concern did not alter the Court's holding in *Smith v. Maryland* when it upheld the warrantless use of a pen register, police have access to vastly more information in cell phones than they do through the use of pen registers.[184] The vast amounts of informa-

176. *See supra* note 98 and accompanying text.

177. *See* Katz v. United States, 389 U.S. 347, 351 (1967); *Quon*, 529 F.3d at 906; United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005). One could also argue that letters should receive greater privacy protections precisely because they are sent with less frequency and one generally does not carry them around on a daily basis. Conceding this, it is still arguable that text messages should be treated differently because the third-party doctrine could easily destroy any expectation of privacy.

178. *See supra* Part II.A. The U.S. Postal Service's fastest guaranteed delivery is Express Mail, or next-day delivery. U.S. Postal Serv., Express Mail Overnight Guaranteed, http://www.usps.com/shipping/expressmail.htm (last visited Jan. 28, 2010).

179. *Compare* United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007) (ignoring the third-party doctrine altogether, focusing on the circumstances surrounding the discovery, and determining that a reasonable expectation of privacy existed), *with Jones*, 149 F. App'x at 959 (applying the third-party doctrine in denying a sender's expectation of privacy in text messages).

180. *See* Jacob Leibenluft, *Do Text Messages Live Forever?*, SLATE, May 1, 2008, http://www.slate.com/id/2190382.

181. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

182. *See supra* Part II.A.

183. *See Finley*, 477 F.3d at 259.

184. Pen register devices reveal only the phone numbers that an individual dials. *Smith*, 442 U.S. at 736 n.1. On the other hand, a police officer searching a mobile phone can discover call records, address books, photos, text messages, e-mail inboxes, music, and more. *See* Stillwagon, *supra* note 165, at 1171–72.

tion stored in modern cell phones entail greater privacy concerns.[185] Therefore, the rationale in *Smith v. Maryland* may not be as applicable to modern cell phones.[186]

Fourth, some privacy protections that exist for senders of letters do not exist for senders of text messages. For example, criminal law distinguishes between letters and text messages by making it a federal offense for anyone other than the addressee to open a letter.[187] In addition, absent some exigency, law enforcement officials must obtain a warrant to open closed packages and sealed letters.[188] Senders of text messages do not enjoy these additional privacy protections. Using the letter analogy to question a sender's reasonable expectation of privacy, while simultaneously denying these additional protections, highly diminishes privacy protections in sending a text message compared with sending a letter. Therefore, the letter analogy results in logical inconsistencies and reduced privacy protections, and thus courts should reexamine using this analogy to determine the validity of a search or seizure of text messages.

2. The Contents of a Container Analogy

Many courts avoid the letter analogy altogether by analogizing the cell phone to a container and text messages to the contents of a container.[189] Consequently, text messages are admitted as evidence against criminal defendants in instances in which the contents of other containers are admitted.[190] Text messages are primarily admitted under the search incident to arrest doctrine.[191]

The container analogy originated with text-enabled pagers.[192] Before widespread use of cell phones, individuals used pagers to send text messages.[193] As a result, the first cases discussing the search and seizure of text messages deal with pagers.[194] For example, in *United States v. Chan*, the defendant's pager revealed information regarding a drug deal.[195] Interestingly, in *Chan*, the defendant himself advocated for the container analogy, arguing that the police needed a search warrant to search its contents.[196] The court responded by accepting Chan's own

185. State v. Smith, No. 2008-1781, 2009 WL 4826991, at *4 (Ohio Dec. 15, 2009). For example, Apple currently offers an iPhone with 32 GB of memory. Apple, *supra* note 24.

186. The Pen Register Act, 18 U.S.C. §§ 3121–3127 (2006), now regulates the use of pen registers.

187. *See supra* note 171 and accompanying text.

188. Walter v. United States, 447 U.S. 649, 656 (1980).

189. *See, e.g.*, United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007).

190. *See id.*

191. *See, e.g.*, *id.* (search incident to arrest); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (search incident to arrest); State v. Novicky, No. A07-0170, 2008 WL 1747805, at *6 (Minn. Ct. App. Apr. 15, 2008) (automobile exception); State v. Smith, No. 07-CA-47, 2008 WL 2861693, at *8 (Ohio Ct. App. July 25, 2008) (search incident to arrest).

192. *See Chan*, 830 F. Supp. at 533.

193. Stillwagon, *supra* note 165, at 1171.

194. *See, e.g.*, *Chan*, 830 F. Supp. at 533; Stillwagon, *supra* note 165, at 1182–83.

195. *Chan*, 830 F. Supp. at 533.

196. *Id.*

analogy without discussion and then denied his motion to suppress under the search incident to arrest doctrine.[197] Most subsequent courts have accepted the analogy wholly with regards to text messages sent via cellular phones.[198]

Addressing the distinction between pagers and cell phones, a few decisions discuss the unique quality of modern cellular phones. One court noted that cell phones, "[u]nlike pagers or address books," "have the capacity for storing immense amounts of private information."[199] As a result, the court granted the defendant's motion to suppress evidence obtained during a post-booking search of a cell phone.[200] The court found that, because of the great quantity of private information stored in cell phones, the police cannot properly search a phone as they can the defendant's clothing during the booking process.[201] In a recent dissenting opinion, an Ohio state appellate judge opined that cellular phones demand greater privacy protections because of their "capacity to store and display great amounts of information: names, phone numbers, addresses, text messages, e-mails, photographs, videos."[202] In December, the Supreme Court of Ohio reversed the appellate court's decision, following the dissent's rationale.[203] Reasoning that cell phones are distinct from other possessions, the dissent at the appellate court level stated, "[t]he divide between the personal computer and the cellular phone appears to be diminishing by the day."[204] Accordingly, there should be some distinction between cell phones and other "containers."

Despite the immense privacy concerns involved with the search of modern cellular phones, many courts, and some commentators, accept the container analogy without comment.[205] As a result, information in a cell phone, including text messages, is admissible under the same circumstances as the contents of a container. For instance, one court justified a station house search of a cell phone under the search incident exception on the grounds that the search was sufficiently contemporaneous with the arrest.[206] Another court, citing *New York v. Belton*,[207] permitted

197. *Id.* at 536.

198. *See* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007); State v. Novicky, No. A07-0170, 2008 WL 1747805, at *4 (Minn. Ct. App. Apr. 15, 2008); State v. Smith, No. 07-CA-47, 2008 WL 2861693, at *5 (Ohio Ct. App. July 25, 2008); Gershowitz, *supra* note 100, at 31. The appellate court's decision in *State v. Smith* was recently reversed specifically because the Supreme Court of Ohio found the container analogy inapplicable to modern cell phones. No. 2008-1781, 2009 WL 4826991, at *4–5 (Ohio Dec. 15, 2009).

199. United States v. Park, No. CR-05-375-SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

200. *Id.* at *1–4.

201. *Id.* at *9.

202. *Smith*, 2008 WL 2861693, at *10 (Donovan, J., dissenting).

203. *Smith*, 2009 WL 4826991, at *4.

204. *Smith*, 2008 WL 2861693, at *10 (Donovan, J., dissenting).

205. *See* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007); State v. Novicky, No. A07-0170, 2008 WL 1747805, at *4 (Minn. Ct. App. Apr. 15, 2008); *Smith*, 2008 WL 2861693, at *5; Gershowitz, *supra* note 100, at 31.

206. *Smith*, 2008 WL 2861693, at *7.

207. *See supra* Part II.D.

the search of a cell phone left charging in the defendant's friend's car.[208] The defendant was sitting on the trunk of his friend's car when the police approached and, according to a witness, the defendant was a recent occupant of the vehicle.[209] Because the cell phone was in police custody for approximately four months prior to the search, invalidating the search incident exception, the court admitted the evidence under the automobile exception.[210]

The Court's decision in *Gant* narrows the circumstances under which searches of containers in vehicles are permissible.[211] For a valid search of a container, the passenger must be "within reaching distance of the passenger compartment at the time of the search" or it must be "reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."[212] The second of the two *Gant* prongs could be carried to the extreme with modern cell phones that carry virtually all of the owner's personal information and communications. The only crimes for which there would perhaps be no evidence contained in a cell phone would be traffic offenses.

Under the twin rationales of the search incident to arrest doctrine—officer safety and the protection of destructible evidence—a search of a cell phone could be justified by the preservation of evidence rationale.[213] Because cell phones are often used in drug deals, a reasonable police officer making a drug arrest could believe the phone contains evidence of a crime.[214] There is a possibility, however remote, that the defendant could access the phone during the arrest and delete incriminating material, satisfying the justification.[215] Before *Gant*, courts generally applied the bright-line rule permitting the search of all containers found in a vehicle if incident to a lawful arrest. This trend is particularly troublesome with cell phones because of the vast amounts of information they can contain.

On at least two occasions prior to *Gant*, however, courts addressed the twin rationales of the search incident doctrine in the context of text messages and found them lacking. In an Ohio state court opinion, a concurring judge applied the exigent circumstances exception in favoring admission of some information discovered on the defendant's cell

208. *Novicky*, 2008 WL 1747805, at *4–5 (citing Thornton v. United States, 541 U.S. 615, 617–18 (2004); New York v. Belton, 453 U.S. 454, 460 (1981)).

209. *Id.* at *2.

210. *Id.* at *6.

211. Arizona v. Gant, 128 S. Ct. 1710, 1719 (2009).

212. *Id.* (internal quotation marks omitted) (quoting *Thornton*, 541 U.S. at 632 (Scalia, J., concurring)).

213. The twin rationales of the search incident exception are officer safety and the preservation of evidence. *See supra* text accompanying note 102. It would be a rare occasion indeed if the search of a cell phone were justified by officer safety. Instances in which the cell phone could potentially be a threat to officer safety (e.g., communicating with a coconspirator or planning an escape) are eliminated by seizure alone.

214. United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009).

215. *See supra* note 113 and accompanying text.

phone.[216] In that case, the trial court only admitted into evidence the phone's call records.[217] The concurring judge stated that "[a] reasonable police officer could conclude that there might be a limit to the number of previous phone numbers contacted on the cell phone, and that the failure to obtain those phone numbers promptly might result in their becoming purged . . . ."[218] The same justification would be true of text messages because some providers purge messages after the inbox reaches a certain limit.[219] Given this explanation, the exigent circumstances exception may be a plausible justification for the warrantless search of a cell phone. This justification is based on the preservation of evidence, but instead of relying on the fiction that an arrestee no longer in possession of a phone can somehow erase valuable information, it relies on the reality that some information stored on cell phones may delete automatically.[220] But as phone memory continues to increase and smart phones become more common, this justification will gradually dissipate.[221]

The search incident to arrest justification also fails when the defendant is arrested on a charge whose proof cannot reasonably be found in a cell phone. Recently, a Florida district court granted the defendant's motion to suppress incriminating photographs found during a warrantless search of his cell phone.[222] The defendant was arrested on the charge of driving on a suspended license.[223] On such a charge, the court found that the twin rationales of the search incident doctrine could not justify the search of defendant's cell phone.[224] The police obtained all the information they needed to charge the defendant by the mere fact that the license was suspended.[225] The subsequent search of the defendant's cell phone was superfluous and unnecessarily invasive.[226] These facts mirror the facts of *Gant*, where the defendant was arrested for driving on a suspended license and handcuffed away from his vehicle before the police

216. State v. Smith, No. 07-CA-47, 2008 WL 2861693, at *8 (Ohio Ct. App. July 25, 2008) (Fain, J., concurring).

217. *Id.*

218. *Id.* Judge Fain did not specifically address his reasons for writing a separate concurring opinion. But because he did not join the majority opinion, which rested on the search incident exception, one may deduce that he found some problem with justifying the warrantless, station house search of a cell phone.

219. *See id.*

220. *See id.*

221. *See* Gershowitz, *supra* note 100, at 29 (describing the capabilities of the new generation of iPhones); Stillwagon, *supra* note 165, at 1172 (referring to the current generation of cell phones as "microcomputers"). Furthermore, in most cases, the law enforcement officer can cure the exigency by turning the phone off. The Court is generally unwilling to deny an exigency, however, merely because there exists a "better way," or when the officer technically had the time or opportunity to get a warrant. *See* Warden v. Hayden, 387 U.S. 294, 298 (1967) (indicating that, even though the police could have taken other actions, a search was valid under the exigent circumstances exception because officers "acted reasonably" in conducting the warrantless search).

222. United States v. Quintana, 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009).

223. *Id.*

224. *Id.*

225. *Id.* at 1298.

226. *Id.* at 1300.

searched the vehicle.[227] In that case, the Court found the fact that Gant was arrested for a traffic offense dispositive in invalidating the preservation of evidence rationale.[228]

3. The Oral Communications Analogy

Analogizing text messages to oral communications better aligns with both common sense and the realities of modern cell phones. Considering text messages and how individuals use them reveals that text messages are more analogous to the oral communications discussed in *Katz* than the contents of a container or letters. In *Katz*, the Court distinguished between "[w]hat a person knowingly exposes to the public" and "what he seeks to preserve as private."[229] The Court declared that the former did not implicate the Fourth Amendment, but the latter "may be constitutionally protected."[230] When law enforcement officers placed a listening device on the outside of Katz's phone booth, the officers "violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[231] What the defendant sought to exclude from the "uninvited ear"—the oral communications spoken into the phone's mouthpiece—was constitutionally protected.[232]

Similarly, senders of text messages have both an objective and subjective expectation of privacy in the messages sent.[233] Text messages are arguably more private than phone conversations, both objectively and subjectively, because they cannot be overheard.[234] The user seeks to exclude the communication from the uninvited ear by avoiding speaking into the mouthpiece altogether.[235] Also, text messages, unlike letters or e-mails, have in the past only been generally accessible through a mobile device.[236] One can make the argument, therefore, that the sender wishes to keep the information especially private by limiting the recipients. Consequently, text messages should be given at least the same protec-

227. Arizona v. Gant, 128 S. Ct. 1710, 1715 (2009).

228. *Id.* at 1719.

229. Katz v. United States, 389 U.S. 347, 351 (1967).

230. *Id.* at 351–52.

231. *Id.* at 353.

232. *Id.* at 352.

233. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906 (9th Cir. 2008) (relying on the operational realities test).

234. Oral communications are still protected under the Fourth Amendment, even if overheard by the government, if the government has to take extreme measures to overhear them. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 506–08 (1961) (inserting a "spike mike" into the walls of an adjoining row house).

235. *Katz*, 389 U.S. at 352. A counterargument is that text messages remain on the recipient's phone. Consequently, unlike a conversation, the message remains there to be shown to or discovered by others.

236. When service providers do keep written archives of text messages, the provisions of the SCA provide additional protections. *See supra* Part II.B. This is also changing with technology that allows access to text messages from computers and allows users to forward text messages to other parties easily.

tions as oral communications because senders have an equally reasonable expectation of privacy in those communications. This reasonable expectation exists unless the recipient voluntarily discloses it to law enforcement.[237]

Accepting that senders of text messages have a reasonable expectation of privacy under the *Katz* test, it is logically inconsistent to subsequently conclude that senders lose that expectation of privacy by transmitting messages through a service provider's network.[238] Justice Marshall made a similar argument regarding the use of pen registers. He stated that "even assuming . . . individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular."[239] In the case of text messages, a cell phone user may know that text messages are sent via the service provider's network, and may know they are stored on the provider's server for some period of time.[240] It does not follow, however, that the user's expectation of privacy in those messages is diminished. This is especially true because text messages are in some ways more private than phone calls or letters.[241] As Justice Marshall stated, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all."[242] The sender's privacy expectation does not disappear completely simply by the nature of the technology.[243]

Commentators have discussed how courts should treat electronic communications in light of *Katz* and its progeny. One view is that a strict reading of *Katz* and *Kyllo* requires greater protections for electronic communications.[244] Another commentator criticizes this "popular view" that "the Fourth Amendment should be interpreted broadly in response to technological change."[245] Professor Kerr argues that law professors and others misconstrue *Katz* and *Kyllo* by focusing on the privacy aspects of the Court's opinion, because the Court's reasoning is dependent on the location of the search.[246] He concludes it is more efficient for the legislature to address privacy concerns raised by electronic communications because the Court's modern trend is not to expand privacy protec-

237. There is no reasonable expectation of privacy under the false friends doctrine if a third party voluntarily discloses information to the government. *See* Hoffa v. United States, 385 U.S. 293, 303 (1966).

238. One who receives a text message can always voluntarily reveal the information to law enforcement. The Fourth Amendment does not protect such information. *See id.*; United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005).

239. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (citation omitted).

240. *See supra* Part II.A.

241. *See* discussion *supra*.

242. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

243. *See id.*

244. *See, e.g.*, Sklansky, *supra* note 58, at 196; Morgan, *supra* note 27, at 828–29.

245. Kerr, *supra* note 13, at 804.

246. *Id.* at 822, 835.

tions generally.[247] In his *Gant* opinion, however, Justice Stevens specifically highlighted the Fourth Amendment's purpose in protecting privacy.[248] Justice Scalia's concurring opinion also stressed that officers arresting an individual "virtually always have a less intrusive . . . means of ensuring their safety" than a search of a vehicle's contents.[249] These opinions indicate that commentators may be mistaken in believing that the current Court is only concerned with privacy when it pertains to the home. The door remains open to protecting cell phones from intrusive, warrantless searches because the technology could allow officers immediate and unfettered access to all of a suspect's personal information.

IV. RECOMMENDATION

This Note suggests that current Fourth Amendment doctrines should permit a fair balancing of a cell phone user's privacy interests with law enforcement interests. The lower courts' use of analogies in analyzing text messages is generally unsatisfactory. Because of the inconsistencies in the letter and container analogies, this Note first recommends viewing text messages as most analogous to oral communications. Yet, this analogy is not perfect because text messages continue to exist in written form, whereas conversations generally do not. The Note then suggests that such analogies may be unnecessary. Utilizing a rule similar to the plain view doctrine, officers may be permitted to search a cell phone provided they have probable cause as to the contents' incriminating nature. Finally, in cases where law enforcement officers reasonably believe it is imperative to search a phone immediately, the search could be justified under exigent circumstances.

Viewing text messages as either letters or contents of a container is inconsistent with current Fourth Amendment jurisprudence. Because Americans communicate electronically more often than they communicate through the post, it is imperative to use an analogy that serves the Fourth Amendment's aim of protecting all individuals' privacy.[250]

Analogizing text messages to letters creates inconsistencies because of the frequency with which texts are sent, the speed of communication, and the comparative lack of protections that are afforded to text messages.[251] Additionally, under the third-party doctrine, a sender loses a reasonable expectation of privacy in at least the number dialed the instant the message is sent.[252] Taken to its logical end, law enforcement agents

247. *Id.* at 888; Kerr, *supra* note 28, at 1242–43.

248. Arizona v. Gant, 128 S. Ct. 1710, 1720 (2009) ("A rule that gives police the power to conduct such a search whenever an individual is caught committing a traffic offence . . . creates a serious and recurring threat to the privacy of countless individuals.").

249. *Id.* at 1724 (Scalia, J., concurring).

250. Draper v. United States, 358 U.S. 307, 314 (1959) (Douglas, J., dissenting) ("[T]he rule we fashion is for the innocent and guilty alike.").

251. *See supra* Part III.C.1.

252. *See supra* notes 62–63 and accompanying text.

may search a cell phone's text and call logs without violating the Fourth Amendment, just as the use of a pen register did not implicate the Fourth Amendment.[253]

Analogizing text messages to the contents of a container is also unsatisfactory.[254] At least one court has held that a search of a cell phone incident to arrest was improper when the individual was arrested for driving on a suspended license.[255] The court reasoned that the dual rationales of search incident to arrest—officer safety and preservation of evidence—were not present and therefore invalidated the search.[256] Moreover, if law enforcement officers can justify the search of a cell phone's contents by analogizing the phone to a container, they have access to potentially vast amounts of information.[257] When the Court developed its bright-line container rules, an individual could not carry thirty-two gigabytes of information on her person.[258] The Supreme Court's opinion in *Gant* indicates that we may be entering an era of returned adherence to the underlying rationales of Fourth Amendment rules.[259] Even so, it is unsatisfactory to think of text messages and other data as "contents" or "objects" that are contained. Rather, this information exists apart from and independently of any one mobile device.

A superior analogy compares text messages with verbal telephone communications. An individual's expectation of privacy in text messages is at least comparable to her expectation of privacy in telephone conversations.[260] Text messages satisfy the *Katz* reasonable expectation of privacy test. First, senders of text messages may have an even greater subjective expectation of privacy than those who use cell phones for verbal communications.[261] The types of messages sent via text evidence a subjective expectation of privacy; in virtually every case dealing with the

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

254. *See supra* Part III.C.2.

255. United States v. Quintana, 594 F. Supp. 2d 1291, 1297 (M.D. Fla. Jan. 20, 2009). In addition, the false friends doctrine would still apply. A defendant cannot prevent another from voluntarily revealing the contents of a text message to the police.

256. *Id.* at 1300. This rationale is questionable even if evidence of the crime could be found in the phone's records. For instance, it is unlikely that a suspect would be able to take out her phone and start manipulating it, with the intent of erasing evidence of a crime, without these actions creating probable cause for seizing the phone. Therefore, there are less intrusive means of getting information relevant to a criminal investigation in this case.

257. *See* Gershowitz, *supra* note 100, at 28.

258. *Cf. supra* note 185. One solution would be legislative action analogous to the Wiretap Act for oral communications. The SCA fails for two reasons: (1) it is out of date with regards to categorizing text messages, and (2) it provides no exclusionary remedy. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900–03 (9th Cir. 2008) (discussing how to characterize text messages under the SCA); Kerr, *supra* note 28, 1242–43.

259. *See supra* notes 211–28 and accompanying text.

260. *See supra* notes 54–56 and accompanying text.

261. *See supra* notes 234–37 and accompanying text. One fictional example of this situation occurred in *The Wire*, mentioned in the Introduction. The drug kingpin communicated with his supplier by pix message to avoid having a conversation intercepted by wiretap. The wiretap equipment could not detect the contents of pix messages, while it could discern the contents of oral communications. *See The Wire: React Quotes*, *supra* note 1.

search of text messages, the messages exposed a drug deal or sexual escapade.[262] Those who send and receive text messages exhibits an expectation of privacy at least comparable to someone using an enclosed payphone.[263] Lower courts addressing the issue found this expectation to be one society also views as reasonable.[264] But this analogy is not ideal. Because text messages continue to exist in a physical sense after transmittal, courts must determine a rule that will govern searches of the physical cell phones. At the same time, because of the potentially immense amount of stored information, it is important to seek a balance between individual privacy and law enforcement.

Following a similar rationale as *Arizona v. Hicks*, courts could permit law enforcement officers to seize a cell phone if they have probable cause to believe it contains evidence of a crime.[265] As a result, police would be able to avoid the risk of destruction of evidence.[266] Law enforcement officers would then be required to particularly describe to a magistrate what evidence they seek during the search—for instance, call log records or text messages that pertain to criminal activity. This would protect the privacy of information that is not relevant to a criminal investigation, and the magistrate would monitor the search of the seized phone.[267]

The probable cause approach would not inhibit law enforcement activities and would be easy to apply by police in the streets. For example, if an officer locates a phone during a search incident to arrest and the crime is one for which communications between coconspirators or codefendants is common, the officer may have probable cause to seize the cell

262. *See, e.g.*, *Quon*, 529 F.3d at 898 (sexually explicit communications); United States v. Finley 477 F.3d 250, 254 & n.2 (5th Cir. 2007) (drug deals); Schaeffer & Elrick, *supra* note 5 (sexually explicit messages).

263. *See* Katz v. United States, 389 U.S. 347, 352 (1967).

264. *See Quon*, 529 F.3d at 905; *Finley*, 477 F.3d at 259.

265. This would essentially be the same standard as the plain view doctrine: an officer has the authority to seize an item if she has probable cause to believe the item is contraband or evidence of a crime. *See* Arizona v. Hicks, 480 U.S. 321, 326 (1987).

266. *See, e.g.*, Steagald v. United States, 451 U.S. 204, 214 n.7 (1981) ("[A]bsent exigent circumstances the magistrate, rather than the police officer, must make the decision that probable cause exists to believe that the person or object to be seized is within a particular place.").

267. *Compare* United States v. Quintana, 594 F. Supp. 2d 1291, 1295–96 (M.D. Fla. 2009) (describing how an officer discovered intimate photos of the defendant and his wife, while searching his cell phone pursuant to a warrantless search), *with* State v. Smith, No. 07-CA-47, 2008 WL 2861693, at *8 (Ohio Ct. App. July 25, 2008) (approving of the trial court's motion to suppress all records that officers did not have "reasonable suspicion was on Smith's person at the time of his arrest" and thus could not have had probable cause to retrieve). This may seem naive because it allows police to describe what they were seeking *post hoc*. The Court's other Fourth Amendment doctrines, however, exhibit a similar need to trust the police to truthfully disclose their reasoning to judges after the fact. For instance, the independent source doctrine allows for the admission of evidence the police would have discovered despite not following proper procedure. Murray v. United States, 487 U.S. 533, 537 (1988). The doctrine relies on police assurances that they did not use illegally obtained evidence to procure a search warrant. *See id.* at 542.

phone.[268] The police may also convince another person, like a codefendant, to voluntarily reveal the contents of text messages.[269]

Lastly, in some cases exigent circumstances may justify an immediate search of a cell phone's contents. This could occur in at least two instances: (1) when an officer is in hot pursuit of a dangerous felon and information in the phone could potentially help locate the felon, and (2) when an officer reasonably believes the contents of the communications in the phone will be lost if the search is delayed.[270] The latter circumstance will diminish as cell phone memories continue to increase. Already it would be difficult to justify search of a PDA, iPhone, or other smart phone using the latter justification because those devices have large memories and generally do not purge messages.[271]

In determining that cell phone users have a reasonable expectation of privacy in text messages, courts should analogize text messages to spoken telephone conversations. Courts should avoid the letter and container analogies altogether. Regarding the search of a suspect's phone for evidence, courts should apply a rule similar to the plain view doctrine; police may search a cell phone if there is probable cause to believe that it contains incriminating evidence. In some limited instances, the exigent circumstances exception may also apply to text message searches.

V. CONCLUSION

Present attempts by lower courts to adapt Fourth Amendment jurisprudence to text messages are contradictory and present as many difficulties as they resolve. Courts should avoid using the letter and container analogies in relation to text messages. The most intuitively satisfactory analogy compares text messages with oral communications. Any analogy would prove unnecessary, however, if courts instead adapt the plain view doctrine to cell phones. Police could conduct warrantless searches of cell phones if they have probable cause to believe that the contents are incriminating. Exigent circumstances also may apply to a warrantless search of a cell phone. This method would balance the competing concerns of individual privacy and effective law enforcement.

268. In addition, the false friends doctrine would still apply. *See supra* note 237.

269. United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005).

270. Both of these instances could fall under an exigent circumstances exception to the warrant requirement. *See Smith*, 2008 WL 2861693, at *8 (Fain, J., concurring) (stating that a warrantless cell phone search would be justified if "a reasonable police officer could conclude that there were exigent circumstances justifying obtaining" information on the phone).

271. *Cf. supra* note 185 and accompanying text.