# Protecting Your Texting: Gaps in Fourth Amendment Protection for Modern Communication

LAUREN HARRIMAN*

## INTRODUCTION

Amy wakes up to her alarm going off. The first thing she does is roll over and checks her phone. She sees a text message from her boyfriend saying, "Good morning beautiful." She replies, "Good morning, see you tonight!" Amy sees another text message from her friend, Sara, "Hey are we still on for lunch at Café Rora?" Amy responds, "Yeah, as long as 12 is okay. I have class and need to be back on campus by 1." Her friend answers, "12 is perfect. I'll see you then." All of these communications occur before Amy even reaches her bathroom, where she also takes her phone to ensure she does not miss any communications.[1]

Once Amy arrives at school, she uses her phone under her desk to sneak texts to her classmates. She also sends another text to her boyfriend, "I bought new underwear for tonight ;)." After meeting Sara for lunch, Amy receives a text from her mother asking how her day is going. Her mother knows better than to try and call Amy—phone calls take time and undivided attention, neither of which Amy has. When Amy sits down to do the homework for her next class, she realizes she forgot to write down the assignment and texts a classmate to ask what it was. Her classmate texts back almost immediately with the assignment.

Once she finishes her homework, Amy drives to meet her brother for dinner. On the way to dinner Amy realizes that she left her phone at home, but does not worry too much because she already confirmed the time and place where she is meeting her brother. Unbeknownst to Amy, her brother possesses a bag full of marijuana he just purchased. Her brother does not have a car, and after dinner Amy offers to drive him home before going to meet her boyfriend. While driving her brother home, a police officer pulls Amy over for speeding. When the officer looks into the car with his flash

* J.D. candidate, University of San Francisco School of Law (2015); B.S. Engineering Physics with a focus in Electronics, Santa Clara University (2010). The Author would like to thank Professor Susan Freiwald and the incredibly talented IPLB editing team for their tireless efforts in editing this Comment, her family for raising her to love technology, and her godparents for inspiring her to study law.

1. *See* Lindsay Goldwert, *Do You Take Your Cell Phone in the Bathroom? 75% of Americans Admit to Calling, Texting on the Toilet*, N.Y. DAILY NEWS (Feb. 2, 2012), http://www.nydailynews.com/life-style/health/cell-phone-bathroom-75-americans-admit-calling-texting-toilet-article-1.1015634 ("Approximately 75% of people take their cell phones into the bathroom with them, according to a survey by the marketing agency 11Mark.... An astonishing 91% of those born between 1977 and 1993 admit to using their phones while seated in the bathroom stall.").

light, her brother neglects to hide the plastic bag containing the marijuana. The officer asks both Amy and her brother to step out of the vehicle, and arrests them for possession of marijuana. Until recently, if the officer found a cell phone on Amy or her brother he would have been able to immediately conduct a search and read through an individual's text messages.[2] Now, the officer must first obtain a warrant.[3]

However, if the officer waits and asks Amy's service provider to turn over all of her stored text messages as part of an investigation into Amy or her brother, the officer can obtain stored text messages dating as far back as the officer desires.[4] Because of this one incident, law enforcement could acquire a record that provides an immense insight into Amy's private daily life.

## I. FOURTH AMENDMENT STANDARDS

### A. STANDARDS THE POLICE USE TO OBTAIN COMMUNICATIONS

Historically, even if the officers had sufficient cause to conduct a search, Amy would not have carried all of her communications with her. For law enforcement to lawfully search and seize any communications—traditionally in the form of letters—it would need to obtain a warrant based on probable cause that identified the communications it was requesting.[5] Probable cause requires that "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[6] It is doubtful that law enforcement could establish sufficient probable cause to obtain a warrant allowing it to search Amy's home from driving her brother home from dinner.[7] Even if law enforcement could obtain a warrant, it would likely not have any reason to believe that Amy's communications

2. On June 25, 2014, the U.S. Supreme Court overruled previous Court of Appeals decisions and held that police must obtain a warrant before searching a suspect's cell phone upon arrest. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014).

3. *Id.*

4. *See infra* Part III.B. This Comment presumes that the presented fact pattern satisfies the standard necessary for law enforcement to obtain an order to compel disclosure.

5. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); Ex parte Jackson, 96 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.").

6. Illinois v. Gates, 462 U.S. 213, 214 (1983).

7. *See* Feliciano v. City of Miami Beach, 847 F. Supp. 2d 1359 (S.D. Fla. 2012). The odor of marijuana emanating from the plaintiff's apartment justified the police's warrantless entry. *Id.* at 1368. The police arrested the plaintiff's boyfriend after observing him in possession of marijuana, but declined to arrest or further search the plaintiff's home. *Id.* at 1369. This suggests that the police were not interested in the plaintiff's potential involvement in her boyfriend's possession of marijuana, and thus had no interest in searching her home. There are several cases where the police had probable cause to search a suspect's vehicle which contained marijuana but declined any attempt to search a suspect's home. *See* United States v. Kellam, 568 F.3d 125, 136 (4th Cir. 2009); State v. Mitchell, 735 S.E.2d 438, 441 (N.C. Ct. App. 2012); United States v. Hernandez-Vargas, CR08-5775RBL, 2009 WL 666867 (W.D. Wash. Mar. 11, 2009), *aff'd*, 387 Fed. App'x 760 (9th Cir. 2010).

contained any evidence pertaining to her brother's marijuana possession. Thus, law enforcement would be unable to seize Amy's communications because its warrant would not have listed such items to be searched and seized.[8]

As communication technologies began to develop, phone calls emerged as the most common form of communication. During that time, phone communications were not stored, so law enforcement could only access those communications by tapping into phone lines and listening in on calls. In order for the government to tap phone lines, it must obtain a wiretap order.[9] A wiretap order is so difficult to obtain that it is commonly known as a "super-warrant."[10] The difficulty can be attributed to the Wiretap Act,[11] which specifies that law enforcement may only obtain a wiretap order when investigating a crime specifically enumerated by the statute.[12]

Additionally, to obtain a warrant the Wiretap Act requires that law enforcement demonstrate necessity as well as satisfy four other elements.[13] To demonstrate necessity law enforcement must have first previously tried and failed to obtain the evidence.[14] Since Amy is not a professional criminal skilled in covert communications, it is doubtful that law enforcement could satisfy the necessity requirement in Amy's case.[15] Thus, the Wiretap Act's listing marijuana possession as one of its enumerate crimes is likely irrelevant for Amy, and during the time when her communications were in the form of phone calls, law enforcement would have been unable to establish the requisite necessity to access her communications via wiretap.[16]

However, not all communications are protected by a warrant

---

8. FED. R. CRIM. P. 41(e)(2)(A) ("Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned.").

9. 18 U.S.C. § 2516(1) (2012).

10. *Wiretapping Law Protects "Oral," "Wire," and "Electronic" Communications Against "Interception,"* ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE PROJECT, https://web.archive.org/web/20131113085930/https://ssd.eff.org/wire/govt/wiretapping-protections (last visited Nov. 30, 2014).

11. 18 U.S.C. § 2510–22 (2012).

12. *Wiretapping Law Protects "Oral," "Wire," and "Electronic" Communications Against "Interception,"* ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE PROJECT, https://web.archive.org/web/20131113085930/https://ssd.eff.org/wire/govt/wiretapping-protections (last visited Nov. 30, 2014).

13. 18 U.S.C. § 2518(1)(c) (2012) ("Each application shall include the following information: . . . a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.").

14. *Id.*

15. For example, law enforcement could follow Amy, and they would eventually find that she makes no effort to cover her tracks--allowing law enforcement to take advantage of her openness and gather evidence.

16. 18 U.S.C. § 2516(1)(e) (2012) (stating that a wiretap order may be approved where the interception of communication may provide evidence of "the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States").

requirement. Lower standards exist that allow the government to obtain certain types of an individual's communications.[17] Differing from the heightened showing of probable cause and necessity standard, law enforcement can obtain a 'D order' based on the "specific and articulable facts" standard.[18] This standard only requires law enforcement show to that Amy's communications are "relevant and material to an ongoing investigation."[19] Law enforcement can prove such relevance by simply showing that the communications have "*any* tendency to prove or disprove a consequential fact."[20] For example, one commentator suggests that if Amy testified in her brother's case, law enforcement could use a court order to obtain Amy's text messages because they would be relevant to her credibility as a witness.[21] Because text messages are the modern equivalent of letters, police violate users' Fourth Amendment rights by relying on a standard that requires only relevance to obtain stored text messages.[22] This Comment argues that a heightened probable cause standard should apply to law enforcement obtaining stored text messages,

B. NOTICE AND SUPPRESSION

The Fourth Amendment explicitly protects communications in letterform.[23] If Amy's communications were letters as opposed to text messages, the Fourth Amendment requires that law enforcement to seek a warrant based on probable cause or ask for Amy's consent before conducting a search.[24] Alternatively, without consent, law enforcement must obtain the warrant and provide Amy a copy of the warrant along with a receipt for any property taken.[25] When phone calls were the primary mode of communication, whether or not a wiretap was approved, law enforcement had to provide notice to the individual and any "such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice" within ninety days, or once any judicially approved extensions terminated.[26]

---

17. 18 U.S.C. § 2703(d) (2012).

18. *Id.* This Comment generally refers to the administrative subpoena created under § 2703(d) as a 'D order.'

19. *Id.*

20. Juan A. Albino, *Do Defendants Have A Privacy Interest in Their Cell Phone's Text Messages and E-Mails?*, 44 REV. JUR. U.I.P.R. 383, 395–96 (2010) (emphasis added).

21. *Id.*

22. Brendan Sasso, *Facebook, Email Providers Say They Require Warrants for Private Data Seizures*, THEHILL (Jan. 25, 2013), http://thehill.com/policy/technology/279441-facebook-email-providers-require-warrant-for-private-data#ixzz320EVAx1P ("'The Fourth Amendment to the U.S. Constitution prohibits unreasonable search and seizure. Law enforcement needs a search warrant to enter your house and seize letters from your filing cabinet . . . .'").

23. U.S. CONST. amend. IV.

24. United States v. Gervato, 474 F.2d 40, 41 (3d Cir. 1973) ("[W]e do not believe that the Fourth Amendment requires the occupant to be present before his home can be searched under a valid search warrant.").

25. FED. R. CRIM. P. 41(f)(1)(C).

26. 18 U.S.C. § 2518(8)(d) (2012); 18 U.S.C. § 2518(1)(f) (2012) (stating that the court must approve requests for extensions).

In addition, for both the seizure of letters and the interception of phone calls, the Fourth Amendment mandates that if law enforcement failed to follow proper procedure the court would suppress any evidence obtained as a result of the flawed warrant.[27] In contrast, the government is not required to give any notice for obtaining stored text messages, and its failure to follow procedure does not lead to the suppression of the text messages.[28]

This Comment discusses the legal hurdles that the government should overcome when they request user's messages from telephone service providers. The government typically requests users' text messages from the service providers when the phone on which the user received the text messages no longer exists or when an individual resists disclosure.[29] Text messages are viewed as one of the most personal methods of modern communication, and the Stored Communications Act (SCA)[30] reflects a pre-modern understanding of electronic communications and provides inadequate protection for text messages.

Part I addresses why users have a reasonable expectation of privacy in their stored text messages, regardless of the application of the Third Party Rule. Part II discusses and proposes amendments to four sections of the SCA. These amendments would accomplish the following: (1) eliminate the definition of remote computing service (RCS) and the 180-day rule, (2) require law enforcement to demonstrate probable cause prior to obtaining text messages, (3) require law enforcement to notify the target of a search or seizure within ninety days, and (4) provide a suppression remedy to deter abuse of the SCA. Part II also assesses two bills currently before Congress that propose amendments the SCA.

## II. FOURTH AMENDMENT PROTECTION FOR TEXT MESSAGES

Text messages are the modern equivalent of the "papers" described and protected by the Fourth Amendment.[31] In terms of communication technology, text messages closely resemble phone calls. However, phone calls are protected by the Wiretap Act, which requires the government to obtain a warrant based on probable cause prior to interception.[32] In contrast to both letters and phone calls, text message users tend to share more of themselves in this form because text messages allow for real time communication.[33] Several studies recognize the immediacy of

27. *See* Johnson v. United States, 333 U.S. 10 (1948); 18 U.S.C. § 2518(10)(a) (2012).

28. *See infra* Part III.C–D.

29. Fred Kemper, *Compulsion of Text Messages After Quon: Applying Old Law to New Technology*, 92 B.U. L. REV. 1381, 1399 (2012) ("Unfortunately, the suspect deleted all messages before the investigators could retrieve them from the phone. The DOJ decides to compel disclosure of any text messages held by the suspect's cellular provider through use of a 2703(d) order, because the DOJ believes that the communications it seeks are in computer storage provided by an RCS.").

30. 18 U.S.C. § 2701–12 (2012).

31. U.S. CONST. amend. IV. *See supra* note 5.

32. *See supra* Part I.A.

33. *Why is Text Messaging so Powerful? Why Use Text Messages?*, THUMBPRINT CITY, http://www.thumbprintcity.com/help/textpower (last visited May 25, 2014) ("Texts are a very personal

communication via text message, and recent court cases and statutes reflect a respect for the role text messaging plays in our daily lives. In light of the special role text messages play in modern society, Congress should extend the Fourth Amendment protections regarding law enforcement access to stored electronic communications.

In *Katz v. United States*,[34] Justice Harlan's concurrence established a two-pronged test for evaluating whether the Fourth Amendment protects a particular type of communication.[35] The test concludes that the Fourth Amendment recognizes a government intrusion as a search when it intrudes into an area in which a person has (1) a subjective expectation of privacy, and (2) society is prepared to accept that expectation of privacy as reasonable.[36]

### A. SUBJECTIVE EXPECTATION OF PRIVACY IN TEXT MESSAGES

Cell phone users are constantly responding to text messages and many communicate highly personal information via those text messages. This pattern of usage demonstrates that people have a subjective belief that those messages will remain private. For example, Amy would not use her phone to send racy messages to her boyfriend if she expected others to be privy to those messages.[37]

#### 1. Studies Show Rapid Response Time to Text Messages

Today "80% of consumers have their cell phones with them at all times."[38] Edge Media,[39] an interactive marketing agency, also reported that the "[a]verage response time to a text message is 5 minutes."[40] CTIA-The Wireless Association,[41] an international nonprofit that advocates for the wireless communications industry, reported an even faster average response time of ninety seconds.[42] HTC, a brand management firm, reported that even during work-hours people expect a reply text from their romantic partner within five minutes.[43] For example, Amy's boyfriend

---

and direct form of communication, and most of the text messages we send and receive in our everyday lives are to close family and friends. This means people will often be very honest in a text message, and say what they need to say, not what they think they should say, even if they would never say those things out loud."). *See supra* Part I.A (explaining why the Fourth Amendment protects letters).

34. 389 U.S. 347 (1967).

35. *Id.* at 361.

36. *Id.*

37. *See* EDGE MEDIA, http://www.edgemedia.biz/index-3.html (last visited Sept. 10, 2014).

38. *Id.*

39. *About Us*, EDGE MEDIA, http://www.edgemedia.biz/index-1.html (last visited Sept. 10, 2014).

40. EDGE MEDIA, http://www.edgemedia.biz/index-3.html (last visited Sept. 10, 2014).

41. *About Us*, CTIA-THE WIRELESS ASS'N, http://www.ctia.org/about-us (last visited Sept. 10, 2014).

42. Patrick Hull, *Why Entrepreneurs Must Have a Mobile Marketing Strategy*, FORBES (Aug. 23, 2013), http://www.forbes.com/sites/patrickhull/2013/08/23/why-entrepreneurs-must-have-a-mobile-marketing-strategy/.

43. HTC Team, *Response-Time Expectations in the Internet Age: How Long is Too Long?*, HTC BLOG (May 27, 2013), http://blog.htc.ca/2013/05/27/response-time-expectations-in-the-internet-age-how-long-is-too-long/.

would never call Amy during the day because he respects her effort to do well in school and refuses to disrupt her classes. However, he would send text messages to Amy and then expect a near immediate response because he believes that text messages are not disruptive. The studies not only demonstrate that text messages are a type of real-time communication, but they also paint a vivid picture of a cell phone bolted to a user's hands.

2. Studies Show that Text Messages are Replacing Phone Calls as the Primary Method of Communication

As of December 2012, U.S. cell phone users per month spent an average total of 187.8 billion minutes talking on the phone,[44] and sent 171.3 billion text messages.[45] Minutes spent on the phone and individual text messages cannot be directly compared, but the statistics at least indicate that for roughly every minute an American spends talking on the phone, another American is sending a text message. Also in 2012, Time Magazine suggested that texting had already surpassed phone calls.[46] In citing the number of text messages U.S. cell phone users sent per month, Time Magazine reported that text messages "exploded from 14 billion in 2000 to 188 billion in 2010," and contended that "[t]he telephone call is a dying institution."[47]

Edge Media reported in 2007 that text message volume exceeded U.S. call volume for the first time in history.[48] Additionally, contrary to popular belief, the primary demographics for texting are not just teenagers, but rather adults ages 18–54.[49] In this Comment's hypothetical, Amy communicates with her mother via text message because the asynchronous nature of text messaging is more convenient than the synchronous nature of a phone call. By texting, Amy could simultaneously communicate with her mother and also do other things. By contrast, Amy is unable to accomplish as much while on a phone call because calls require more focus and attention.[50] Modern cell phone users' increasing inclination to text logically shows that users like Amy have a reasonable expectation that their text messages are just as private as phone calls. In light of this modern trend and expectation, text messages deserve to have the same level of protection

44. Lauren Sherman, *Dear Everyone: Never Call Me Again*, ELLE (Apr. 4, 2014), http://www.elle.com/life-love/society-career/why-i-hate-talking-on-the-phone.

45. *2014 Distracted Driving Awareness Month Key Facts & Statistics*, CAL. OFFICE OF TRAFFIC SAFETY, http://www.ots.ca.gov/pdf/campaign/2014_Distracted_Driving_Fact_Sheet.pdf (last visited Nov. 30, 2014).

46. Jeffrey Kluger, *We Never Talk Anymore: The Problem with Text Messaging*, TIME (Aug. 16, 2012), http://techland.time.com/2012/08/16/we-never-talk-anymore-the-problem-with-text-messaging/ ("Americans ages 18–29 send and receive an average of nearly 88 text messages per day, compared to 17 phone calls.").

47. *Id.*

48. EDGE MEDIA, http://www.edgemedia.biz/index-3.html (last visited Sept. 10, 2014).

49. *Id.*

50. Kluger, *supra* note 46 ("[Texting] meant a conversation I could control—utterly. I get to say exactly what I want exactly when I want to say it. It consumes no more time than I want it to and, to a much greater degree than is possible with a phone call, I get to decide if it takes place at all. That might make me misanthropic. It surely makes me a crank. But it doesn't make me unusual.").

as phone calls.

3. Text Messages are Personal

In 2012, Harris, a market research firm, conducted a poll, which found that one out of five Americans 'sexts.'[51] McAfee, a computer virus protection company, released a report in February of 2014 finding that "half of adults' phones contain 'sexting' content."[52] This information indicates that Amy's conduct of sending highly personal sexual text messages is normal behavior. Stored text message content is personal because it can paint a vivid picture of a user's day. For example, text message content may include an individual's thoughts, feelings, plans, and even sexual desires.

It is unclear for how long service providers store text message content. Many sources cite to documents obtained by the American Civil Liberties Union (ACLU), which suggest that cell service providers typically do not store text message content, and if they do, it is only held for a limited period of time.[53] However, when a woman accused basketball star Kobe Bryant of rape, the District Court in Colorado had the unique opportunity to discover how long AT&T actually stores text message content.[54] USA Today reported that District Judge Terry Ruckriegle of Colorado reviewed at least four months worth of the women's text messages, which Bryant's attorneys subpoenaed in an effort to prove the sexual relations were consensual.[55]

AT&T and Verizon currently offer technology that allows users to store multiple months worth of text messages.[56] Both providers also

---

51. Sara Gates, *Adult Sexting On The Rise: 1 in 5 Americans Send Explicit Text Messages, Poll Finds*, HUFFINGTON POST (June 8, 2012), http://www.huffingtonpost.com/2012/06/08/adult-sexting_n_1581234.html; *Sexting Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/sexting (last visited May 19, 2014) (defining 'sexting' as "the sending of sexually explicit messages or images by cell phone").

52. Julianne Pepitone, *Scandalous Stats: Half of Adults' Phones Contain 'Sexting' Content*, NBC NEWS (Feb. 14, 2014), http://www.nbcnews.com/tech/mobile/scandalous-stats-half-adults-phones-contain-sexting-content-n22121.

53. *See* Darlene Storm, *How Long Does Your Mobile Phone Provider Store Data for Law Enforcement Access?*, COMPUTERWORLD BLOGS (Sept. 28, 2011), http://blogs.computerworld.com/19016/how_long_does_your_mobile_phone_provider_store_data_for_law_enforcement_access; David Kravets, *Which Telecoms Store Your Data the Longest? Secret Memo Tells All*, WIRED (Sept. 28, 2011), http://www.wired.com/2011/09/cellular-customer-data/; Declan McCullagh, *Cops to Congress: We Need Logs of Americans' Text Messages*, CNET (Dec. 3, 2012), http://www.cnet.com/news/cops-to-congress-we-need-logs-of-americans-text-messages/.

54. Jon Sarche, *Text Messages May Turn Up in Kobe Bryant Case*, USA TODAY (June 7, 2004), http://usatoday30.usatoday.com/tech/news/techpolicy/2004-06-07-bryant-text-msgs_x.htm.

55. *Id.*

56. *See AT&T Messages*, AT&T, http://www.att.com/shop/apps/att-messages.html?source=IAMS2500000000ZCU#fbid=RcxeiUny0xv (last visited Dec. 1, 2014) (stating that AT&T's messaging services stores texts, call logs, and voicemails on the cloud so that they are available via web and tablet); *Verizon Messages FAQ*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/verizon-messages.html (last visited Dec. 1, 2014) (stating under the dropdown link titled "How long are messages stored using Integrated Messaging with Verizon Wireless Message +?" that the Integrated Messaging service syncs ninety days of messages between the web and a user's iPhone, tablet, or other devices); Lance Ulanoff, *Messages Can Be Forever*, PCMAG (Aug. 11, 2004), http://www.pcmag.com/article2/0,2817,1634503,00.asp.

recently began offering an application that enables users to read their text messages on tablet devices.[57] However, in order to access their text messages on the tablets, both AT&T and Verizon require users to allow the service provider to backup the text messages on the service providers' servers.[58] Furthermore, both providers tout this backup requirement as a positive feature by celebrating each applications' capability to store text and picture messages for longer periods of time.[59] Beyond the providers' positive words, it is clear that both providers have the capability to store text messages for enormous amounts of time—supporting the evidence provided in the Kobe Bryant case rather than the documents obtained by the ACLU.

If and when a user realizes that this practice is a massive invasion of privacy, both AT&T and Verizon can disable the automatic backup feature.[60] However, both companies warn users that they will lose the ability to access their text messages on the tablet devices.[61] The requirement that users permit their service provider to retain sensitive communications contradicts the notion that users voluntarily convey their text messages to their service provider.[62]

B. OBJECTIVE EXPECTATIONS OF PRIVACY

New statutes and case law show Congress and the courts progressing towards explicitly protecting users' text message privacy.[63] For example,

---

57. *AT&T Messages*, AT&T, http://www.att.com/shop/apps/att-messages.html?source=IAMS2500000000ZCU#fbid=RcxeiUny0xv (last visited Dec. 1, 2014); *Verizon Messages FAQ*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/verizon-messages.html (last visited Dec. 1, 2014).

58. *AT&T Messages*, AT&T, http://www.att.com/shop/apps/att-messages.html?source=IAMS2500000000ZCU#fbid=RcxeiUny0xv (last visited Dec. 1, 2014); *Verizon Messages FAQ*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/verizon-messages.html (last visited Dec. 1, 2014).

59. *AT&T Messages*, AT&T, http://www.att.com/shop/apps/att-messages.html?source=IAMS2500000000ZCU#fbid=RcxeiUny0xv (last visited Dec. 1, 2014); *Verizon Messages FAQ*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/verizon-messages.html (last visited Dec. 1, 2014).

60. *AT&T Messages*, AT&T, http://www.att.com/shop/apps/att-messages.html?source=IAMS2500000000ZCU#fbid=RcxeiUny0xv (last visited Dec. 1, 2014); *Verizon Messages FAQ*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/verizon-messages.html (last visited Dec. 1, 2014).

61. *AT&T Messages: FAQs*, AT&T, http://www.att.com/shop/apps/att-messages.html#fbid=RcxeiUny0xv (last visited Dec.1, 2014) ("If you remove the network storage service, text messages, call logs, and voicemails will no longer be accessible from your tablet or on the Web."); *Verizon Messages FAQ*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/verizon-messages.html (last visited Dec. 1, 2014) ("[Y]ou must subscribe to the Integrated Messaging service if you want to access your messages from your tablet.").

62. *See infra* Part II.B.5.i.

63. The progress that Congress and the Courts are making is possibly motivated by studies showing that the public is prepared to accept users' subjective expectation of privacy in their text messages. *See* Henry F. Fradella, Weston J. Morrow, Ryan G. Fischer & Connie Ireland, *Quantifying*

the Telephone Consumer Protection Act (TCPA) acknowledges that users actually read all of their text messages, and permitting unsolicited text messages by spammers invade users' privacy.[64] Additionally, the court in *State v. Clampitt* rejected the notion that the Fourth Amendment does not protect information revealed to a third party (the "Third Party Rule").[65] Furthermore, the court in *State v. Bone* overturned its precedent, holding that users maintain a reasonable expectation of privacy in the content of their text messages.[66] These decisions reflect that the Third Party Rule is an outdated understanding of stored communications such as text messages.

1. The Telephone Consumer Protection Act

The TCPA protects users from unsolicited telephone calls and text messages, but its coverage does not extend to unsolicited e-mails.[67] This suggests that Congress regards text messages as similar to phone calls. The reasoning behind the prohibition of making unsolicited cell phone calls and sending unsolicited text messages was that historically users paid per minute for cell phone usage, and also paid per text message sent. Today, this pay structure is only seen in relation to data usage, but some wireless carriers still have plans where users pay up to $0.20 for an individual text message, and the price increases if they attach a picture.[68] These fees can quickly pile up when users send numerous text messages within a given month.[69]

---

Katz: *Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 358 (2011) (Nearly 58% of the survey participants agreed that "[w]hen teenagers take digital pictures of themselves naked and send them to other teenagers using the multimedia text messaging service of a cell phone, they should . . . expect those photos to be kept private. Thus, if the pictures are discovered by school officials and/or police (who have no warrant to search the contents of a cell phone), the photos should nonetheless [not] be admissible in an criminal prosecution for having transmitted images that might legally constitute child pornography.").

64. 47 U.S.C. § 227(a)(4) (2012) (stating that the definition of telephone solicitation applies to telephone calls or messages). "Over seven years ago the Federal Communications Commission (FCC) explicitly stated that the TCPA's prohibition on automatic telephone dialing systems "encompasses both voice calls and text calls to wireless numbers including, for example, short message service (SMS) calls . . . ." In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 18 F.C.C.R. 14014, 14115 (2003). In *Kramer v. Autobytel, Inc.*, the United States District Court for the Northern District of California found that, "[i]n 2009, early in the time period during which [the defendant] allegedly received the unsolicited text messages, the Ninth Circuit held unambiguously that a text message is a 'call' for purposes of the TCPA." Kramer v. Autobytel, Inc., 759 F. Supp. 2d 1165, 1169–70 (N.D. Cal. 2010).

65. State v. Clampitt, 364 S.W.3d 605, 611 (Mo. Ct. App. 2012); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the Fourth Amendment does not prohibit the obtaining of information revealed to a third-party and conveyed by him to Government authorities, 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).

66. State v. Bone, 107 So. 3d 49, 66 (La. Ct. App. 2012).

67. 47 U.S.C. § 227 (2012).

68. Verizon charges $.20 per text sent and $.25 per picture, video, and voice message sent. *About Our Messaging Packages*, VERIZON WIRELESS, https://www.verizonwireless.com/b2c/store/planMessagingOverlay.jsp (last visited Dec. 1, 2014).

69. Since cell phone users between the ages of eighteen and twenty-four exchange roughly 4,000 texts per month, if those users did not have a text message plan the monthly bill could be around $800. Alex Cocotas, *CHART OF THE DAY: Kids Send A Mind Boggling Number Of Texts Every Month*, BUSINESS INSIDER (Mar. 22, 2013), http://www.businessinsider.com/chart-of-the-day-number-of-texts-sent-2013-3#ixzz32s4Io9E8. However, most service providers now offer unlimited texting for under $100 per month, and instead focus on charging users for data usage. *See About Our Messaging*

Imagine if users received text message spam to the extent that most people receive e-mail spam. Not only would the majority of text messaging costs be spent on unsolicited messages, but individuals would also have to spend time sifting through mountains of unsolicited text messages. If the ability to block text messages were limited there would be no effective way to gain control over text messaging costs.[70] Congress recognized the severe harm that text spam could cause users, and criminalized such actions.[71] By enacting the TCPA Congress demonstrated its understanding that a text messages is a highly personal communications tool, and cell phone users only expect to receive text messages from people with whom they are already familiar. Courts could rely on this appreciation to interpret the TCPA as signifying Congress's acceptance of a user's reasonable subjective expectation of privacy in their text messages.

2. *State v. Clampitt*

The court in *State v. Clampitt* held that the Third Party Rule does not nullify a user's expectation of privacy in the content of text messages that are accessible by their service provider.[72] More importantly, the court explicitly recognized an objective expectation of privacy in the content of text messages.[73] After charging the defendant, James Clampitt, with first-degree involuntary manslaughter and leaving the scene of a motor vehicle accident, police obtained the defendant's text messages from his service provider.[74] The police hoped to obtain evidence from Clampitt's text messages that he or a member of his family was driving the vehicle involved in the accident.[75] The special prosecutor obtained four investigative subpoenas to obtain the contents of Clampitt's text messages spanning over various timeframes.[76] The special prosecutor relied on the authority of investigative subpoenas rather than a properly executed search warrant because she believed that the Third-Party Rule precluded Clampitt's text messages stored by a third-party service provider from Fourth Amendment protections.[77]

The *Clampitt* court found that "[t]he rationale used by the *Warshak* court in establishing individuals' reasonable expectations of privacy in the

---

*Packages*, VERIZON WIRELESS, https://www.verizonwireless.com/b2c/store/planMessagingOverlay.jsp (last visited Dec. 1, 2014); Jared Newman, *Which Wireless Plan Is Cheapest?*, TIME (Feb. 14, 2014), http://time.com/7982/which-wireless-plan-is-cheapest/.

70. For example, Verizon allows users to block certain numbers, but the blocks expire every ninety days, and users can only block up to five numbers. *Spam Control FAQs*, VERIZON WIRELESS, http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/spam_controls.html (last visited May 25, 2014).

71. Courts have upheld 47 U.S.C. § 227(a)(4) against First Amendment challenges. *See, e.g.*, Accounting Outsourcing, LLC. v. Verizon Wireless Pers. Commc'ns, L.P., 329 F. Supp. 2d 789, 818 (M.D. La. 2004). The court in *Accounting Outsourcing, LLC v. Verizon Wireless Pers. Commc'ns, L.P.*, additionally upheld the TCPA's lack of scienter. *Id.* at 812.

72. State v. Clampitt, 364 S.W.3d 605, 611 (Mo. Ct. App. 2012).

73. *Id.*

74. *Id.* at 607.

75. *Id.* at 608.

76. *Id.* at 612.

77. *Id.* at 608.

contents of their email is equally applicable to cell phone users' expectation of privacy in the contents of their text messages."[78] In *United States v. Warshak*, the court addressed "whether law enforcement officers violated the defendant's Fourth Amendment rights by obtaining the content of the defendant's emails from his Internet service provider ("ISP") without a warrant."[79] The *Clampitt* court's reference to *Warshak* seems to suggest that individuals still have a reasonable expectation of privacy in their text messages despite being stored with a third-party service provider, and the Fourth Amendment protects to such contents. The *Clampitt* court's holding, in addition to many other courts' decisions[80] evidence courts' desire to "apply the *Warshak* court's view on emerging technology and the Fourth Amendment."[81]

The *Clampitt* court explained that just because service providers may access users' text messages does not mean that the messages are not private, thereby rejecting the Third Party Rule.[82] Most importantly, the court expressed that "[w]hat individuals once communicated through phone calls and letters can now be sent in a text message," and there is "no reason why the same information communicated textually from that same device should receive any less protection under the Fourth Amendment."[83] The *Clampitt* court therefore concluded that "as text messaging becomes an ever-increasing substitute for the more traditional forms of communication, it follows that *society expects* the contents of text messages to receive the same Fourth Amendment protections afforded to letters and phone calls."[84]

3. *State v. Bone*

The court in *State v. Bone* held that the defendant, Bone, had a

78. *Id.* at 611.

79. *Id.* at 610 (citing United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that e-mails are communications subject to Fourth Amendment protections)).

80. *See* United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (holding that a person does not automatically lose her expectation of privacy regarding her e-mails when she logs onto a public network); R.S. v. Minnewaska, No. 12-588 (MJD/LIB), 2012 WL 3870868 (D. Minn. Sept. 6, 2012) (holding that a student had a reasonable expectation of privacy for private information on a social network account); In the Matter of Applications for Search Warrants for Info. Associated with Target Email Address, No. 12-MJ-8119-DJW, 2012 WL 4383917 (D. Kan. Sept. 21, 2012) (upholding an individual's Fourth Amendment right to e-mails stored on an ISP and denying a search warrant that asserted otherwise); *Clampitt*, 364 S.W.3d at 605 (finding that the defendant had an expectation of privacy for sent text messages even though they were confiscated on another phone). *But see* State v. Hinton, 280 P.3d 476 (Wash. Ct. App. 2012) (holding that the defendant did not have an expectation of privacy in sent text messages); Evan Peters, *The Technology We Exalt Today Is Everyman's Master*, 44 WASH. U. J.L. & POL'Y 103, 131 n.187 (2014).

81. Peters, *supra* note 80, at 131.

82. In contrast, many courts have recognized the Third Party Rule. *Id.* at 120 n.108 (citing United States v. Suarez-Blanca, No. 07-CR-0023-NHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (finding no privacy interest in historical cell site information); United States v. Hynson, No. 05-576, 2007 WL 2692327, at *5 (E.D. Pa. Sept. 11, 2007) (cell phone records); United States v. Phibbs, 999 F.2d 1053, 1077–78 (6th Cir. 1993) (credit card statements); United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *1–2 (9th Cir. Aug. 24, 1992) (kilowatt consumption from electric utility records); United States v. Willis, 759 F.2d 1486, 1489 (11th Cir. 1985) (motel registration records); United States v. Hamilton, 434 F. Supp. 2d 974, 979 (D. Or. 2006) (employment records)).

83. *Clampitt*, 364 S.W.3d at 611.

84. *Id.*

reasonable expectation of privacy in his text messages and therefore law enforcement must establish probable cause before they could collect and review the content of his text messages from his service provider.[85] The police initiated an investigation against Bone when it learned from multiple witnesses that his vehicle was involved in a gang shooting.[86] The police used a subpoena to obtain his text messages from his service provider, which provided substantial evidence for the investigation.[87] Bone's cell phone was his personal device, although the documented subscriber and owner was his mother.[88] In determining whether Bone exhibited a reasonable expectation of privacy in his text messages, the court declined to consider the fact that a few of Bone's text messages stated that he could not talk on his phone because law enforcement had his number.[89]

The *Bone* court agreed with the holding in *Clampitt*, finding that where text messages are sent and received for personal reasons, a user has a reasonable expectation of privacy in those text messages.[90] Without evaluating whether society was prepared to recognize as reasonable users' subjective expectation of privacy in text messages, the court ruled that law enforcement must show probable cause before reviewing personal text messages.[91] The court's simple deferral to *Clampitt*'s holding and lack of further analysis seems to suggest that a user's subjective expectation of privacy in text messages is so reasonable that the second prong of the reasonable expectation of privacy test is not even worth analyzing.[92]

4. The Ninth Circuit's Analysis in *Quon v. Arch Wireless Operating Co., Inc.*[93]

The Ninth Circuit in *Quon v. Arch Wireless Operating Co.*, analyzed an employee's reasonable expectation of privacy in text messages sent on work-related devices.[94] The defendant, Quon, was a police officer working for the city of Ontario (the "City").[95] The City maintained a written policy regarding officers' use of the department's computer, Internet, and e-mail system limiting any use to City-related business, and gave officers notice that it reserved the right to monitor all usage.[96] When the City acquired pagers for its officers to use, it announced that it considered pager messages to be akin to e-mail, thus making pager messages subject to

85. State v. Bone, 107 So. 3d 49, 66 (La. Ct. App. 2012).

86. *Id.* at 53.

87. *Id.* at 54.

88. *Id.*

89. *Id.* at 61.

90. *Id.* at 66.

91. *Id.*

92. *Id.* at 67.

93. 529 F.3d 892, 906 (9th Cir. 2008), *rev'd sub nom.* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

94. *Quon*, 529 F.3d at 907.

95. *Id.* at 895.

96. *Id.* at 896.

audit.[97] However, the lieutenant in charge of Quon's pager expressed that he would not audit officers' messages so long as the officer paid any applicable overage fees.[98] Quon exceeded his monthly text character allotment multiple times, but always paid the overage fee and, as promised, the lieutenant did not audit his messages.[99] Without notice to his officers, the lieutenant complained to his superior that he was tired of being a bill collector.[100] In response, the superior ordered him to request pager message transcripts for the pagers that regularly exceeded their character allotment.[101] The transcripts revealed that Quon exceeded his 25,000-character allotment by 15,158 characters, and used his pager to send personal messages that were often sexually explicit.[102]

*Quon* presented two scenarios where users should have a reasonable expectation of privacy in their text messages: (1) where users did not expect to have their text messages audited,[103] and (2) where the communications were personal regardless of the workplace setting.[104]

The *Quon* court held that when employees have reason to rely on an established policy regarding electronic communication, that policy is controlling.[105] The court recognized that Quon had signed the document dictating the department's general policy regarding the use of the department's computer, Internet, and e-mail systems, and he was present at the meeting where the department informed officers that pager messages were subject to audit.[106] However, the court found that the "operational reality" of the policy controlled the expectation.[107] The operational reality of the policy was that when Quon repeatedly exceeded his character allotment, the lieutenant simply collected the overage charges without auditing his messages.[108] This routine evidenced the department's intent to follow its own informal policy, and the officers reasonably relied on such policy.[109] The court concluded that because Quon had reasonably relied on the informal policy, he "had a reasonable expectation of privacy in the text messages archived on Arch Wireless's server."[110] On appeal, the Supreme Court avoided the analysis of the operational reality, and instead assumed several propositions *arguendo*, including that Quon had a reasonable

97. *Id.*
98. *Id.* at 897.
99. *Id.*
100. *Id.*
101. *Id.* at 897–98.
102. *Id.* at 898.
103. *Id.* at 906.
104. *Id.* at 908.
105. *Id.* at 907.
106. *Id.* at 906.
107. *Id.* at 907.
108. *Id.*
109. *Id.*
110. *Id.*

expectation of privacy in his text messages.[111]

Applying the Ninth Circuit's operational realities reasoning to cell service providers, if a service provider does not lead users to believe that it will audit its users' text messages, the users should have a reasonable expectation of privacy in the messages stored on the service providers' servers. With the exception of T-Mobile, none of the major cell service providers give users reason to believe that they engage in auditing practices.[112] Moreover, Sprint expressly agrees to not "look at" users' text messages.[113] Thus, users maintain a reasonable expectation of privacy because they generally have no reason to believe their service provider will audit the content of their text messages.[114]

With respect to personal communications, the Ninth Circuit held that even employees whose employers record their phone calls have a reasonable expectation of privacy in those personal calls, and the court used that analysis to reject the City's argument that the California Public Records Act[115] (CPRA) defeated Quon's reasonable expectation of privacy in his text messages.[116] The *Quon* court concluded that public record requests could only defeat a reasonable expectation of privacy where the

111. City of Ontario, Cal. v. Quon, 560 U.S. 746, 760 (2010).

112. *See* Stephen Lawson, *Who's Been Reading My Cell-phone Records?*, PCWORLD (Nov. 25, 2008), http://www.pcworld.com/article/154536/privacy_cell_records.html (stating that Verizon employees were put on paid leave when Verizon wireless discovered that "some employees viewed information from an Obama cell-phone account that has been discontinued for several months . . . [i]nformation that is saved by mobile operators . . . includes . . . text messages" implicates that it is not Verizon Wireless's policy for employees to audit users' text messages). AT&T's privacy policy and Code of Business Conduct say very little about AT&T's use of users' content. *See AT&T Privacy Policy*, AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Oct. 4, 2014); *AT&T's Code of Business Conduct*, AT&T 1, 6 (2014), http://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf. The section of AT&T's privacy policy regarding information it collects only mentions the number of text messages sent and received, and states that AT&T will use that information only to improve user experience, to make its business stronger, and lists several examples of what that means. *See AT&T Privacy Policy*, AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Oct. 4, 2014). AT&T's Code of Business Conduct states, "We protect the privacy of our customers' communications." *AT&T's Code of Business Conduct*, AT&T 1, 6 (2014), http://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf. MetroPCS's privacy policy states that MetroPCS captures text messages, but in the section explaining how MetroPCS uses information collected, there is no reference to reading text messages content. *See MetroPCS Privacy Policy*, METROPCS (Dec. 20, 2013), http://www.metropcs.com/metro/tac/termsAndConditions.jsp?terms=MetroPCS%20Terms%20and%20Conditions%20of%20Service. Sprint's privacy policy states, "Sprint has not and will not look at or share text messages, personal information or emails." *Customer Privacy FAQs*, SPRINT NEWSROOM (May 20, 2014), http://newsroom.sprint.com/consumer-resources/customer-privacy-faqs.htm. *But see T-Mobile Privacy Policy Highlights*, T-MOBILE, https://www.t-mobile.com/company/website/privacypolicy.aspx (last updated Dec. 30, 2013) ("[S]ome of the ways we may automatically collect information include . . . captur[ing] details about . . . text messages you send and receive.").

113. *Customer Privacy FAQs*, SPRINT NEWSROOM (May 20, 2014), http://newsroom.sprint.com/consumer-resources/customer-privacy-faqs.htm ("Sprint has not and will not look at or share text messages, personal information or emails.").

114. *See Quon*, 529 F.3d at 906.

115. CAL. GOV. CODE § 6250–6276.48.

116. The City of Ontario argued that, "Quon had no reasonable expectation of privacy because, under that Act, 'public records are open to inspection at all times . . . and every person has a right to inspect any public record.'" *Quon*, 529 F.3d at 907 (quoting CAL. GOV'T CODE § 6253).

requests are "so widespread or frequent as to constitute 'an open atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable.'"[117] Additionally, the court concluded that "the fact that a hypothetical member of the public may request Quon's text messages . . . d[id] not make his belief in the privacy of [his] text messages objectively unreasonable."[118] On appeal, the Supreme Court narrowed the Ninth Circuit's conclusion by finding that even assuming that Quon had a reasonable expectation of privacy "it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny."[119] The Ninth Circuit's rule has wide ramifications because it provides users an instant reasonable expectation of privacy where they believe their text messages are personal.

Though the Supreme Court did not address what role operational realities play, and failed to narrowly define Quon's reasonable expectation of privacy, the Ninth Circuit's analysis indicates progress towards accepting users' reasonable expectation of privacy in the content of their text messages.

5. The Third Party Rule Does Not Apply To Text Messaging

The Third Party Rule stems from the Supreme Court case *United States v. Miller*.[120] In *Miller*, law enforcement obtained Miller's business records using only a subpoena, despite the bank having maintained the records in compliance with the Bank Secrecy Act.[121] The *Miller* Court created a narrow exception to the Fourth Amendment protection by classifying Miller's documents as ordinary business records of the Bank and not his personal confidential communications.[122] However, three years later in *Smith v. Maryland*,[123] the Court referenced *Miller* and several previous cases to broaden the Third Party Rule and claim it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[124] The Third Party Rule enumerated in *Smith* dictates that once users turn over their information to a third party, the Fourth Amendment no longer protects it from investigation, and the government can obtain a subpoena to access such information from the third party.[125] Currently, courts consider both the *Miller* and *Smith* versions of the Third Party Rule.[126] However, the Court in

117. *Id.* at 907.

118. *Id.* at 907–08.

119. City of Ontario, Cal. v. Quon, 560 U.S. 746, 762 (2010).

120. 425 U.S. 435 (1976).

121. *Id.* at 436; *see also* Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114-2.

122. *Miller*, 425 U.S. at 442.

123. 442 U.S. 735 (1979).

124. *Id.* at 743–44.

125. *Id.* at 744 (citing *Miller*, 425 U.S. at 443).

126. *See In re* United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010). The case addressed the Third Party Rule apart from *Miller* and separately from *Smith*. *Id.* ("*Miller* and *Smith* do not permit warrantless law enforcement access to all historical cell site data, because the user has not 'knowingly exposed' or 'voluntarily conveyed' that information to the

*Smith* established a broad version of the Third Party Rule that is not sufficient for modern society where users have no choice but to convey the content of their text messages to third parties. Instead, the analysis provided in *Warshak* ultimately rejecting the Third Party Rule should be expanded to cover text messages.

i. Voluntarily Conveying Communications Does Not Equate to Giving Consent

The Court's broad interpretation of the Third Party Rule in *Smith* was based on the assumption that users voluntarily convey their information to a third party.[127] But courts should no longer make this assumption. Modern users do not voluntarily convey communications to third parties just as someone suffering a heart attack is not considered to consent to emergency medical care.[128] Participation in contemporary society requires the use of modern communication methods.[129] These methods of communication—including text messaging—necessitate users to convey information to third parties.[130] It is illogical for courts to deem a conveyance as voluntary, when users have no alternative options and must convey all communications through third parties.[131]

Society rejects the notion that users truly consent to conveying their communications to third parties. Professor Marc McAllister conducted a survey which empirically proved that society does not believe that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and therefore "assumes the risk" of disclosure to the government."[132] In light of this, Greg Nojeim, Senior Counsel at the Center for Democracy and Technology, contends that the Third Party Rule "rests on a false notion of consent," and users' conveyance to third parties is really more "akin to compelled consent, which is not consent at all."[133] If courts accepted these arguments, users would then retain the appropriate Fourth Amendment protections because courts would recognize the legitimate expectation of privacy in their communications even after the communications are conveyed to third

provider, as those phrases are ordinarily understood. Historical cell site data are not ordinary business records of the providers.").

127. *Smith*, 442 U.S. at 744.

128. *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 68 (2011) (equating third parties who maintain account content with other necessary services such as medical or legal services).

129. *Id.* at 78 ("Where the societal norms and technological norms dictate that third parties must manage more qualitatively and quantitatively personal information, the doctrinal contours of the third-party doctrine must be reinterpreted.").

130. *Id.* at 73–74.

131. Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA JOURNAL (Aug. 1, 2012), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/; Ghoshray, *supra* note 128, at 36 ("[T]he role of a third party as a technology enabler has become necessary in post-modern communication.").

132. Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 498 (2012).

133. Nojeim, *supra* note 131.

parties.

ii. Applying *Warshak*'s Reasoning Leads to the Conclusion That the Third Party Rule Does Not Apply to Text Messages[134]

The court in *Warshak* had a rare opportunity to influence how the Third Party Rule applies to modern communication. In *Warshak*, the plaintiff, Warshak, sought to enjoin the government from obtaining his stored e-mail messages from his service provider without first obtaining a warrant.[135] By analyzing the service provider's right to access the communications and distinguishing personal communications from the bank records in *Miller*, the plaintiff succeeded in dissuading the court from applying the Third Party Rule to e-mail communications.[136]

The *Warshak* court rejected the argument that a third party's "mere *ability* . . . to access the contents of a communication [was] sufficient to extinguish a reasonable expectation of privacy."[137] The court also analogized e-mails to letters and phone calls explaining that a third party's right to access e-mails does not extinguish the Fourth Amendment right in such communications.[138] The court gathered additional support for its conclusion by analyzing the Fourth Amendment's application to rented space.[139] The cases pertaining to rented space supported finding a reasonable expectation of privacy in situations where maids have a right of access, and where landlords can access their tenants' apartments.[140] "[R]outine access is hardly dispositive with respect to the privacy question."[141]

The *Warshak* court's analysis is directly applicable to stored text messages because, according to the SCA, e-mails and text messages are simply "contents of . . . electronic communications in electronic storage,"[142] and are therefore treated interchangeably. Thus, a service provider's right to access the contents of user's stored text messages does not negate a user's reasonable expectation of privacy in that content. Directly addressing *Miller*, the *Warshak* court rejected the application of the Third Party Rule for two reasons. First, the court found that the e-mails

134. United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010) (explaining that regardless of whether a third-party has the right to monitor content the degree of access does not diminish the reasonableness of the plaintiff's expectation of privacy in his e-mails).

135. Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-Mail: The Law Professors' Brief in* Warshak v. United States, 41 U.S.F. L. REV. 559, 560 (2007).

136. *Warshak*, 631 F.3d at 287–88.

137. *Id.* at 286.

138. *Id.* at 287 ("[T]he ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country."). Analogizing to the phone calls discussed in *Katz*, the *Warshak* court explained that, while the language in the e-mail service provider's policy tracked the language in the phone service provider in *Katz*, the right of access did not diminish any reasonable expectation of privacy. *Id.* (discussing Katz v. United States, 389 U.S. 347 (1967)).

139. *Id.*

140. *Id.*

141. *Id.*

142. 18 U.S.C. § 2703 (2012).

at issue were not ordinary business records.[143] Second, the court distinguished between communications sent to a service provider versus those sent through the provider.[144]

a. Confidential Communications: Ordinary Business Records v. Text Messages

The *Warshak* court held that the e-mails in question were a "potentially unlimited variety of 'confidential communications,'" and therefore not ordinary business records like the documents at issue in *Miller*.[145] Under this rule, where a communication is not an ordinary business record, users do not forfeit their reasonable expectation of privacy by conveying the communication to a third party. Professor Susan Freiwald further explained that the Court in *Miller* did not rule that Miller forfeited his reasonable expectation of privacy in his bank records by conveying them to his bank.[146] The Court rather had to "examine the nature of the particular documents sought to be protected in order to determine whether there [wa]s a legitimate 'expectation of privacy' concerning their contents."[147] Professor Freiwald argues that this rule extends to cell site location information[148] because it contains "extensive personal information," and it "much more closely resembles the private communications the *Miller* Court found subject to a reasonable expectation of privacy than the banking records it did not."[149] Following the *Miller* Court and Professor Freiwald's reasoning, users do not forfeit their reasonable expectation of privacy when they convey their text messages to a service provider because text messages contain extensive personal information.

b. Intermediary v. Intended Recipient

The *Warshak* court additionally found that the third party in question, Warshak's service provider, was acting merely as an intermediary and was not the intended recipient of the communications.[150] The court therefore concluded that Warshak intended to send his e-mail *through* his service provider and not *to* the provider.[151] By contrast, the *Miller* Court held that Miller voluntarily conveyed his information to the third party in question, his bank, in order for the bank to use the information in the "ordinary course of business."[152] The *Warshak* court's ruling has gained little traction

143. *Warshak*, 631 F.3d at 288.

144. *Id.*

145. *Id.*

146. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 734 (2011).

147. United States v. Miller, 425 U.S. 435, 442 (1976).

148. Freiwald, *supra* note 146, at 678–79 (stating that the records of the cell towers with which a mobile phone communicates and provides a phone's physical location is considered cell site location information).

149. *Id.* at 734–35.

150. *Warshak*, 631 F.3d at 288.

151. *Id.*

152. *Id.*

in other courts. But by comparing e-mails to letters and ISPs to post offices, the court's use of analogy allows for the conclusion that contacting the ISPs to obtain the contents of e-mails is the equivalent of "storm[ing] the post office and intercept[ing] a letter."[153] Accordingly, the court required that law enforcement obtain a warrant before contacting the ISPs.[154]

While the court's comparison of e-mails to letters is an imperfect analogy because the post office does not retain a copy of the letters it sends, the root of *Warshak*'s reasoning perfectly describes the role of service provider intermediaries. An intermediary is never the intended recipient of an e-mail, and as such, has no right to view the contents of the message let alone the right to turn over its contents to police without being presented with a warrant. Cell service providers serve the same role as the ISP in *Warshak* because text messages are not sent to the service provider. Consequently, the Third Party Rule should not apply, and law enforcement should be required to obtain a warrant before compelling disclosure of stored text messages.

## III. STATUTORY PROTECTION FOR TEXT MESSAGES

In 1986, Congress enacted the SCA to outline the proper procedure for law enforcement if they needed to gain access to stored electronic communications.[155] With the SCA, Congress targeted multiple types of stored communications and based protections upon the type of service provided and the length of time the communication was in storage.[156] As it stands, the SCA inadequately protects text messages, and Congress should amend its provisions. Currently, two bills are before Congress that incorporate adequate amendments. This Comment identifies four critical problems with the SCA's protection of text messages: (1) the SCA relies on outdated definitions of service providers; (2) the variety of procedural hurdles law enforcement must surmount results in confusion and uncertainty; (3) users have difficulty challenging any law enforcement abuse of the SCA due to the potential for indefinite notification; and (4) the SCA's lack of an evidentiary suppression remedy makes challenging law enforcement abuse of the SCA futile.

### A. OUTDATED DEFINITIONS OF SERVICES COVERED BY THE SCA LEAVE TEXT MESSAGES VULNERABLE

Most stored text message content falls under 18 U.S.C. § 2703(b)(1)(B)(ii), which covers communications sent through remote computing services (RCS).[157] This section applies to stored text message

153. *Id.* at 286.

154. *Id.*

155. Kimberly S. Cuccia, *Have You Seen My Inbox? Government Oversteps the Fourth Amendment Again: Goodbye Telephones, Hello E-Mail*, 43 VAL. U. L. REV. 671, 699 (2009).

156. *Id.*

157. 18 U.S.C. § 2703(b)(1)(B)(ii) (2012) ("A governmental entity may require a provider of

content because users read the vast majority of the text messages they receive.[158] But stored text messages could also potentially fall under the provisions governing electronic communication services (ECS).[159] When stored text messages are classified as communications facilitated by an ECS, law enforcement must obtain a warrant before compelling disclosure if the text messages are less than 180 days old.[160] However, the SCA considers text messages that are stored longer than 180 days as abandoned, and law enforcement may obtain these with only a court issued subpoena.[161] The 180-day rule and separate definitions for ECS and RCS made sense in 1986, when connection to service providers was cost prohibitive and it forced users to download local copies of their electronic messages, but now text message service providers encourage users to back-up their text messages to the cloud.[162] In light of modern technology, the SCA's arbitrary categorization of service providers and outdated notion of abandonment is troublesome and lends itself to the creation of arbitrary rules surrounding the procedural hurdles law enforcement must surmount to access stored text messages.

Both the Yoder-Polis and Leahy-Lee SCA amendment proposals properly address amending the definition section of the SCA and the 180-day rule.[163] Rather than redefining ECS and RCS, both bills propose to replace ECS with electronic communication service or remote computing service,[164] thereby extending the protections the SCA formerly afford only to ECS. Additionally, both bills recognize that the 180-day rule is confusing and outdated, and propose to remove it.[165] If Congress implements either bill, it would be a great stride towards updating the SCA

---

remote computing service to disclose the contents of any . . . electronic communication . . . with prior notice from the governmental entity to the subscriber or customer if the governmental entity . . . obtains a court order for such disclosure under subsection (d) of this section."); *see also* 18 U.S.C. § 2711(2) (2012) (defining remote computing service as entities that provide to the public "computer storage or processing services by means of an electronic communications system").

158. The court "ultimately concluded the messages were discoverable and that the service was most likely acting as an RCS once the stored messages had been received." Eric R. Hinz, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 507 (2012) (discussing Flagg v. City of Detroit, 715 F.3d 165 (6th Cir. 2013)). *See supra* Part II.B for evidence of rapid response time, suggesting users read most of their text messages.

159. *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 902 (9th Cir. 2008) ("[I]t is clear that the [text] messages were archived for 'backup protection' . . . . Accordingly, Arch Wireless is more appropriately categorized as an ECS than an RCS."); 18 U.S.C. § 2510(15) (2012) (defining electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

160. 18 U.S.C. § 2703(a) (2012).

161. *Id.*

162. *See supra* Part II.A.3 (discussing cloud backup required for accessing text messages on a user's tablet).

163. Email Privacy Act, H.R. 1852, 113th Cong. (2013); Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013).

164. Email Privacy Act, H.R. 1852, 113th Cong. (2013); Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013).

165. Summary of the Electronic Communications Privacy Act Amendments Act of 2013, PATRICK LEAHY: U.S. SENATOR FOR VT, http://www.leahy.senate.gov/download/section-by-section-ecpa-reform-bill (last visited May 21, 2014).

to adequately protect text messages.

### B. LAW ENFORCEMENT SHOULD NEED TO PRESENT PROBABLE CAUSE BEFORE OBTAINING TEXT MESSAGE CONTENT

Subsection (d) of 18 U.S.C. § 2703 in the SCA allows law enforcement to obtain stored text messages with only a court order.[166] The court order, or 'D order,' "may be issued by any court that is a court of competent jurisdiction," and the court shall issue the order if law enforcement presents "specific and articulable facts showing that there are reasonable grounds to believe that the contents [of stored text messages] . . . are relevant and material to an ongoing criminal investigation."[167] The language stating that the court "shall issue" the order indicates that the court is required issue the 'D order' whenever law enforcement satisfies the "specific and articulable facts" standard.

The "specific and articulable" standard is convoluted and difficult for both scholars and courts to properly define.[168] Professor Christopher Slobogin explains that "the specific and articulable facts need only to support a finding that the information is relevant and material to an ongoing investigation. Relevance and materiality in evidence law is not hard to satisfy, and merely means that the evidence be logically related to a proposition in the case."[169] Thus, obtaining a 'D order' is not a significant challenge for law enforcement.

Law enforcement should be required to demonstrate probable cause prior to obtaining the content of an individual's text messages. Amending the SCA to require probable cause would bring it closer towards complying with the Fourth Amendment. The Yoder-Polis and Leahy-Lee bills both propose to amend the SCA by requiring a warrant based on probable cause before the police may compel the disclosure of text messages.[170] These bills would provide better protections in accordance to the modern text message user's expectations and would make the SCA much easier for the courts and law enforcement to understand.[171] While both bills have significant bipartisan support in Congress, neither has made any headway in over a year.[172]

---

166. 18 U.S.C. § 2703(b)(1)(B)(ii) (2012).

167. *Id.* § 2703(d).

168. *See* Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 161 (2005).

169. *Id.* at 162 ("[A] § 2703(d) order, like a subpoena, allows accessing any records that might be relevant to an investigation, not just the target's."). *See supra* Part I.A. (providing additional information regarding the specific and articulable standard).

170. Email Privacy Act, H.R. 1852, 113th Cong. (2013); Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013).

171. *See supra* Part II.B.

172. Press Release, Mike Lee, U.S. Senator for Utah, Senate Judiciary Committee Approves Leahy-Lee Electronic Communications Privacy Amendments Act (Apr. 25, 2013), http://www.lee.senate.gov/public/index.cfm/press-releases?ID=e42ba48d-66e3-4f20-ae5a-bf7c51ea5916 ("The Leahy-Lee ECPA Amendments Act of 2013 is truly bipartisan in nature. It enjoys broad support from the technology industry, privacy advocates, constitutional scholars, and policy

C. THE SCA MUST PROVIDE VICTIMS THE OPPORTUNITY TO CHALLENGE SCA ABUSES

The potential for indefinite delay of notification to users impedes users' ability to challenge law enforcement for abusing the SCA. Section 2703(b)(1)(B)(ii) states "delayed notice may be given pursuant to section 2705."[173] Under § 2705, law enforcement's court order application can request an order delaying notification to the target of the investigation for up to ninety days if the court determines that there is reason to believe notification will result in: "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial."[174]

Section 2703(d) permits law enforcement to keep surveillance orders secret long after an investigation is over. For investigations showing that a suspect is innocent, that suspect will never know that law enforcement obtained their text messages.[175] According to Magistrate Judge Stephen Smith:

> The default rule is that a 2703(d) order will not be sealed . . . in many districts the government routinely avoids these weaker SCA secrecy provisions by the simple expedient of combining its requests for a 2703(d) order and a pen/trap order into a single application and order. The combined order is then automatically sealed and gagged by authority of the Pen/Trap Statute. Although neither statute appears to contemplate such combined orders, no published court opinion has challenged the practice.[176]

Further, Judge Smith explains that when an order is temporarily sealed, the court rarely unseals it later on, making the seal generally permanent.[177] Thus, if Amy was cleared of any wrong doing in relation to her brother's drug possession arrest, so long as law enforcement does not find any additional evidence that Amy was involved in another criminal act, she would likely never know that law enforcement obtained her stored text messages from her service provider. Congress must amend subsection (d) to only allow one request by law enforcement to delay notification. Both the Yoder-Polis[178] and Leahy-Lee[179] bills fail to eliminate the potential for indefinite delay of notification. Instead, they propose to

---

groups on both ends of the ideological spectrum. I'm grateful to Chairman Leahy's leadership on this issue and I urge my colleagues on both sides of the aisle to support this legislation."); Press Release, U.S. Representative Jared Polis, Polis Becomes Lead Democrat on Email Privacy Act (May 23, 2013), http://polis.house.gov/news/documentsingle.aspx?DocumentID=335412 ("Since introducing the legislation last week, Rep. Polis has worked with Reps. Yoder and Graves to gather a total of 77 co-sponsors for the bill.").

173. 18 U.S.C. § 2703(b)(1)(B)(ii) (2012).

174. 18 U.S.C. § 2705(a)(2) (2012).

175. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. J.L. & POL'Y 313, 315 (2012).

176. *Id.* at 325.

177. *Id.*

178. Email Privacy Act, H.R. 1852, 113th Cong., at 8 (2013).

179. Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong., at 10 (2013).

partially amend subsection (d). Both bills require that police apply to the court for each extension. Though the amendments are an improvement, users continue to lack the opportunity to challenge governmental abuses of the SCA.

### D. THE SCA MUST PROVIDE INCENTIVE FOR VICTIMS TO DIRECTLY CHALLENGE SCA ABUSES

A suppression remedy is a statutorily created solution derived from the exclusionary rule that allows courts to prevent juries from considering evidence that was improperly obtained by law enforcement.[180] Congress's failure to provide a suppression remedy in the SCA "furnishes little incentive for defendants to bring statutory claims against law enforcement acquisition of their electronic communications," leaving "[t]he government's compliance with the Internet surveillance laws [to] remain unexamined" by the courts."[181] If nothing else, "[a] suppression remedy would deter abuses of the [SCA] by law enforcement officials."[182] Unfortunately, neither the Yoder-Polis nor the Leahy-Lee bills address this gap in the SCA's protection of text messages. Another bill, introduced by Senator Wyden and Representative Chaffetz may include a suppression remedy, but that proposal only targets a user's geolocation data rather than text message content.[183]

## CONCLUSION

The standards set by the Fourth Amendment for searches and seizures are the appropriate standards for protecting stored text messages. Not only do text messages users exhibit a subjective reasonable expectation of privacy in their text messages, but court decisions and recent statutory proposals also demonstrate that society recognizes those expectations as objectively reasonable. To better protect stored text messages, Congress must amend the SCA to reflect the Fourth Amendment requirements and force law enforcement to obtain a warrant based on probable cause prior to compelling message content. Furthermore, Congress should redefine "service provider" to encompass both communication services and remote computing services, remove the 180-day rule, amend ability to delay notification, and add a statutory suppression remedy. These amendments would update the SCA to better reflect modern text messaging practices,

---

180. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("[A]ll evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court.").

181. Freiwald, *supra* note 146, at 681; Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 806–07 (2003).

182. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1436 (2004).

183. Nate Cardozo & Mark Jaycox, *Even Attorney General Eric Holder Supports ECPA Reform*, ELEC. FRONTIER FOUND. (May 23, 2013), https://www.eff.org/deeplinks/2013/05/even-attorney-general-eric-holder-supports-ecpa-reform.

and ensure that people like Amy maintain their constitutional right of privacy.