Volume 61
Issue 6 *V.61, Tolle Lege*

Article 2

6-15-2017

Don't Press Send: Commonwealth V. Diego Takes Reasonable Expectation Of Privacy Away From Texters

Marc B. Robertson

DON'T PRESS SEND: *COMMONWEALTH V. DIEGO* TAKES REASONABLE EXPECTATION OF PRIVACY AWAY FROM TEXTERS

MARC B. ROBERTSON*

"[W]e as human beings, even those of us who in words disclaim the importance of our own privacy, instinctively understand the profound importance of it."[1]

I. YOU HAVE ONE NEW MESSAGE: AN INTRODUCTION TO THE PENNSYLVANIA SUPERIOR COURT'S MESSAGE THAT TEXTS ARE NOT PRIVATE

As presidential candidates Rand Paul and Chris Christie stood on the debate stage, they sparred over one of the most pressing and contentious matters facing the United States today: the government's invasion of individuals' privacy rights.[2] Christie, a former United States Attorney and strong supporter of law enforcement, argued for continuing the use of mass surveillance in an effort to prevent terrorist attacks.[3] Paul, a libertarian and staunch opponent of government surveillance, provided a familiar retort to each of Christie's comments: "Get a warrant!"[4] The issue these two men were debating was whether the warnings from George Orwell's dystopian commentary *1984* were coming true: "There was of course no way of knowing whether you were being watched at any given moment. . . . You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."[5]

* J.D. Candidate, 2017, Villanova University Charles Widger School of Law; B.A. 2012, Villanova University. I would like to thank my family and friends who continue to support me throughout all my endeavors. I am especially grateful to those who provided feedback and input in writing this Note. I would also like to thank the *Villanova Law Review* and everyone whose work went into publication of this Note.

1. Glenn Greenwald, *Why Privacy Matters*, TED TALKS (Oct. 7, 2014), transcript *available at* www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript?language=en [https://perma.cc/UY3W-F5FM] (discussing concerns over privacy issues in wake of Edward Snowden revealing details about government's mass surveillance programs).

2. *See Transcript: Read the Full Text of the Primetime Republican Debate*, TIME (Aug. 6, 2015), http://time.com/3988276/republican-debate-primetime-transcript-full-text/ [https://perma.cc/DV85-YNS5] (updated Aug. 11, 2015, 4:30 PM) (responding to question regarding government surveillance).

3. *See id.*

4. *See id.*

5. *See* GEORGE ORWELL, 1984, at 3 (1st Signet Classic reprt. 1961) (1949). *See generally*, Greenwald, *supra* note 1 (referencing George Orwell's discussion of surveillance activities of Big Brother in novel 1984). In his recent TED Talk, Mr. Greenwald addresses the issue of privacy in the wake of revelations by Edward Snowden that the American government was involved in "indiscriminate surveillance." *See id.* Early in the lecture, he addresses the argument made by many in support of this surveillance that "no real harm [] comes from this large-scale invasion because only people who are engaged in bad acts have a reason to want to hide and to care about their privacy." *See id.* Greenwald, however, rebukes

While terrorist attacks and mass indiscriminate surveillance are more extreme circumstances than those at issue in *Commonwealth v. Diego*,[6] the superior court decision could have far-reaching and potentially grave ramifications on privacy in the Commonwealth of Pennsylvania.[7] In *Diego*, Curtis Doval Diego set up a drug transaction via text message with a police informant.[8] After his arrest, Diego argued he had a reasonable expectation of privacy in the text messages sent to the informant and that the police violated the Wiretapping and Electronic Surveillance Control Act (the Pennsylvania Wiretap Act) by "intercept[ing]" his text messages without first obtaining a warrant.[9] Upon review of the trial court decision to suppress the evidence, the superior court found Diego lacked a reasonable expectation of privacy in the text messages he sent.[10] Because of this, there was no "interception" of those messages as the informant voluntarily turned them over to law enforcement.[11]

This Note argues that Pennsylvania courts ought to recognize a reasonable expectation of privacy in text messages.[12] Further, the Pennsylvania legislature should amend the Pennsylvania Wiretap Act to address the Pennsylvania Superior Court's decision in *Diego* and require law enforcement to obtain a warrant before obtaining an individual's text messages, even if the recipient of those messages relays them to the police.[13] Part II provides a background of privacy issues in the United States.[14] Next, Part III sets out the facts and procedure of *Diego*.[15] Part IV then analyzes the superior court's reasoning.[16]

---

this notion, stating that although there are people who claim to not care about privacy, no one truly feels this way. *See id.* He says that all human beings "instinctively understand the profound importance of [privacy]." *Id.* Greenwald believes that all humans "crave[]" privacy and notes that many psychological studies have found that when people believe they are being watched, they change their behavior "dramatically." *See id.* He notes that government access to items humans believe should be private harms society as a whole. *See id.* This issue is extremely important to humans because,

> [I]t is a realm of privacy, the ability to go somewhere where we can think and reason and interact and speak without the judgmental eyes of others being cast upon us, in which creativity and exploration and dissent exclusively reside, and that is the reason why, when we allow a society to exist in which we're subject to constant monitoring, we allow the essence of human freedom to be severely crippled.

Id.

6. 119 A.3d 370 (Pa. Super. Ct. 2015), *appeal denied*, 129 A.3d 1240 (Pa. 2015) (mem.) (unpublished table decision).

7. For a thorough discussion of the impact of the *Diego* decision, see *infra* notes 126–58 and accompanying text.

8. *See Diego*, 119 A.3d at 372–73 (discussing police use of informant to set up drug transaction).

9. *See id.*

10. *See id.* at 372 (reversing suppression order).

11. *See id.* at 382 (holding that trial court decision should be overturned).

12. For a further discussion of the need for courts to find a reasonable expectation of privacy in text messages, see *infra* notes 133–47 and accompanying text.

13. *See Diego* at 380–81 (finding no interception occurs in violation of Pennsylvania Wiretap Act when informant "voluntarily" relays text messages to law enforcement officer).

14. For a further discussion of privacy issues, see *infra* notes 18–78 and accompanying text.

15. For a further discussion of the facts, procedural history, and holding in *Diego*, see *infra* notes 79–125 and accompanying text.

16. For a further discussion of the need for a broader expectation of privacy and

Part V concludes by arguing for a broader expectation of privacy in sent text messages and asserting the Pennsylvania Wiretap Act should be amended to close the loophole that allows law enforcement officers to obtain text messages from an informant without obtaining a warrant.[17]

II. FROM PAGERS TO FLIP PHONES TO SMART PHONES: A BACKGROUND OF LEGAL DECISIONS REGARDING PRIVACY IN TECHNOLOGY

As technological developments have led to new and different varieties of communication, courts have been faced with the issue of deciding what is private and what is not.[18] These cases typically involve the Fourth Amendment to the United States Constitution and address the issue of whether law enforcement must obtain a warrant before searching one's property.[19] As technology has advanced, state surveillance statutes such as the Pennsylvania Wiretap Act have come under review, and courts have had to balance privacy issues against the ability of law enforcement to fight crime.[20] While the law is

---

legislation to protect that privacy, see *infra* notes 126–58 and accompanying text.

17. For a discussion of how *Diego* may affect privacy rights in the future, see *infra* notes 159–63 and accompanying text.

18. *See* City of Ontario, v. Quon, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."); *see also* Joseph C. Vitale, Note, *Text Me Maybe?:* State v. Hinton *and the Possibility of Fourth Amendment Protections over Sent Text Messages Stored in Another's Cell Phone*, 58 ST. LOUIS L.J. 1109, 1110 (2014) (explaining that recent Supreme Court decisions on this issue have given broad deference to lower courts to decide cell phone privacy issues). For a detailed account of the development of cell phones and text messaging technology, see Vitale, *supra*, at 1112–18 (detailing cell phone use around world). Vitale notes that cell phones are "one of the most rapidly growing new technologies in the world." *Id.* at 1112 (quoting Mikiyasu Hakoama & Shotaro Hakoyama, *The Impact of Cell Phone Use on Social Networking and Development Among College Students*, 15 AM. ASS'N BEHAV. & SOC. SCI. J., Spring 2011, at 1, 2) (internal quotation marks omitted). Because cell phones are widely used, people have grown attached to their cell phones. *See id.* at 1113–14. Due to this attachment, studies have found that most people consider the information stored on their cell phones to be private. *See id.* Vitale also provides several interesting statistics regarding cell phone privacy, including,

> [s]eventy-eight percent of Americans consider the information on their cell phones to be "at least as private as that on their home computers." Furthermore, nearly 20% of Americans think their cell phones hold more private information than do their computers. Seventy-six percent of Americans think that law enforcement officers should need permission from a court before searching the cell phone of "a person arrested on suspicion of committing a crime, if the person does not consent to having the phone searched."

Id. at 1114 (footnotes omitted) (quoting Jennifer M. Urban, Chris Jay Hoofnagle & Su Li, *Mobile Phones and Privacy* 2 (UC Berkeley Public Law Research Paper No. 2103405, 2012), *available at* http://ssrn.com/abstract=2103405)). Vitale further discusses the history of text messages and writes that today, text messaging (in addition to taking photos) is the most commonly used function of cell phone owners. *See id.* at 1116–17. These statistics indicate that courts will need to address the issue of privacy in text messaging, as it is now so widespread. *See id.* 1112–18.

19. For a discussion of the Fourth Amendment and the use of warrants, see *infra* notes 23–28 and accompanying text.

20. For a thorough discussion of the Pennsylvania Wiretap Act, see *infra* notes 29–37

unsettled regarding an expectation of privacy when sending a text message, a growing trend signals greater privacy rights in the future.[21] The Pennsylvania legislature must recognize these privacy rights and will need to address loopholes like those in the Pennsylvania Wiretap Act, which allow police officers to access text messages relayed by informants without obtaining a warrant.[22]

A. *Passcode Required: The Fourth Amendment and the Supreme Court's View of a Reasonable Expectation of Privacy*

In order to search and seize an object or document, law enforcement must abide by the Fourth Amendment, which typically involves obtaining a warrant.[23] There are situations, however, where a warrantless search may be

---

and accompanying text.

21. *See, e.g.*, *Quon*, 560 U.S. at 760 (discussing pervasiveness of cell phones). The Court in *Quon* considered that because cell phones and text messages were so widely used, this may "strengthen the case for an expectation of privacy." *See id.* While the Court considered that Quon may have had a reasonable expectation of privacy in his text messages, because the City owned the device, and because of the "'special needs' of the workplace," it was appropriate for the police department to require access to the messages in certain situations. *See id.* at 760–61; *see also* State v. Hinton, 319 P.3d 9, 15 (Wash. 2014) (en banc) (holding that individual who shares information with another party does not lose expectation of privacy); John Soma, Melodi Mosley Gates & Michael Smith, *Bit-Wise but Privacy Foolish: Smarter E-Messaging Technologies Call for a Return to Core Privacy Principles*, 20 ALB. L.J. SCI. & TECH. 487, 503–04 (2010) (discussing society's views on e-messaging technologies and privacy interests). In discussing trends in technology and privacy, the authors argue that users

> base[] [their] expectation of privacy on how [they] use[] the technology, such as to carry on a conversation, rather than on the specific technical means used. This functional view by users lends credence to the idea that society should—and likely will—recognize a reasonable expectation of privacy for e-messaging.

Id. at 504.

22. *See* Soma et al., *supra* note 21, at 518 ("Uncertainty in the law leaves e-messaging users . . . without clear guidance . . . ."). Soma, Gates, and Smith note that courts have shown willingness to "a privacy principle-based approach . . . regarding text messages," but the law regarding this privacy is very unclear. *See id.* at 517–18; *see also* Lathrop B. Nelson, III, *Don't Text with an Informant and iPads Are Not Phones*, WHITE COLLAR ALERT (June 25, 2015), http://whitecollarblog.mmwr.com/tag/commonwealth-v-diego/ [https://perma.cc/U5K5-CYZU] (reviewing Pennsylvania Superior Court decision in *Diego*). Nelson argues that *Diego* will force citizens to be "vigilant" to avoid government overreaching, rather than requiring the government to uphold its constitutional obligations. *See id.*

23. *See* U.S. CONST. amend. IV. The Fourth Amendment states:

> 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.

Id.; *see also* Vitale, *supra* note 18, at 1118–19 & n.60 (discussing search and seizure requirements under Fourth Amendment). In analyzing cell phone privacy, many courts analogize cell phones to "wallets, address books, and diaries." *See id.* at 1122. Because cell phones have address books, and because police are "entitled to open a pocket diary to copy the owner's address," some courts have found that police should be entitled to "turn on a cell

reasonable.[24] If a government official or law enforcement officer violates the Fourth Amendment and performs an illegal search and seizure, the defendant can, under certain circumstances, have that evidence suppressed.[25] In addressing whether there is a reasonable expectation of privacy in text messages, many courts have looked to the Supreme Court's decision in *Katz v. United States*.[26] In his concurring opinion, Justice Harlan laid out a test for determining whether an individual has a reasonable expectation of privacy, which has been frequently invoked in subsequent court decisions.[27] Justice Harlan's two part test requires "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[28]

---

phone to learn its number." *See id.* (internal quotation marks omitted). However, courts have begun to recognize a distinction between a cell phone number and the "highly private" information that can be found on a modern cell phone. *See id.*

24. *See* 18 PA. CONS. STAT. § 5704(2)(ii) (2015) (noting exception to warrant requirement of Pennsylvania Wiretap Act when one party gives consent prior to interception); *see also* Vitale, *supra* note 18, at 1118-19 (discussing that there are "various exceptions" to warrant requirement of Fourth Amendment).

25. *See* Vitale, *supra* note 18, at 1118–19 (discussing exclusionary rule). Not only is illegally-obtained evidence suppressed in such situations, any evidence that was "[the] exploitation of that illegality" is also suppressed. *Id.* at 1119 n.65 (alteration in original) (quoting Wong Sun v. United States, 371 U.S. 471, 488 (1963) (discussing "fruit of the poisonous tree" doctrine)) (internal quotation marks omitted).

26. 389 U.S. 347 (1967).

27. *See id.* at 361 (Harlan, J., concurring) (introducing test for reasonable expectation of privacy).

28. *See id.* (creating test for reasonable expectation of privacy). It is important to note that there are some exceptions to the *Katz* test. These include what a person knowingly exposes to the public, the "misplaced trust doctrine," when a person sends a letter, and exigent circumstances. *See* Vitale, *supra*, note 18, at 1120 (discussing exceptions to *Katz* test whereby one has no reasonable expectation of privacy). Under the misplaced trust doctrine, "people place their trust in others at their own peril and must assume the risk of [that] betrayal." *Id.* at 1120 (alteration in original) (quoting DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 82, 107 (3d ed. 2011)) (internal quotation marks omitted). Further, when a person knowingly exposes information to the public, that information is not protected by the Fourth Amendment. *See id.* Among the examples of public disclosure that forecloses Fourth Amendment protection, courts have decided that when a person sends a letter, there is no expectation of privacy in the contents once the intended party receives it. *See id.* at 1140–41 (discussing letter doctrine). Finally, in exigent circumstances, warrantless searches may be lawful if the need for law enforcement is greater than the privacy interests. *See id.* at 1120–21. These include "life-threatening exigencies, hot pursuit, and preservation of evidence from destruction." *Id.* at 1121 (quoting Clifford S. Fishman, *Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1, 13 (1987)) (internal quotation marks omitted). Often, courts have allowed for warrantless searches of cell phones in an effort to preserve evidence. *See id.* at 1121–22. However, some courts—notably the Ohio Supreme Court—have rejected this rationale, claiming that service providers may maintain cell phone records and law enforcement may be able to obtain a warrant to search those records. *See id.*

B. *Mark as Read: Overview of Pennsylvania's Wiretapping and Electronic Surveillance Control Act*

The Pennsylvania Wiretap Act is a state statute that seeks to protect citizens from illegal wiretaps that violate the Fourth Amendment.[29] While states have the freedom to adopt their own legislation, they must do so in accordance with federal law and provide at least the same amount of protection as the federal law.[30] Under the Pennsylvania Wiretap Act, it is illegal to intentionally "intercept[] . . . disclose[] . . . or . . . use[] the contents of any wire, electronic or oral communication . . . ."[31] Pennsylvania courts have consistently held that the purpose of the Pennsylvania Wiretap Act is to ensure the protection of privacy, and therefore courts have strictly construed the provisions of the Act.[32]

Generally, a person has a reasonable expectation of privacy during an oral conversation, but there has been disagreement over whether one has a reasonable expectation of privacy in other forms of communication, such as emails.[33] Another source of confusion often occurs when courts attempt to

---

29. *See* 18 PA. CONST. STAT. §§ 5701–5782 (1978); *see also* Commonwealth v. Deck, 954 A.2d 603, 607–10 (Pa. Super. Ct. 2008) (discussing purpose of Pennsylvania Wiretap Act). In reviewing the statute, the court instructed, "[The Pennsylvania] Wiretap Act is modeled on Title III ('Title III') of the Omnibus Crime Control and Safe Streets Act of 1968" which "authorizes states to adopt wiretap statutes that trigger greater, but not lesser, protection than that available under federal law." *Id.* at 607. Further, the court instructed that the provisions of the statute must be "construed strictly" in an effort to protect privacy interests. *See id.*

30. *See* Commonwealth v. Birdseye, 670 A.2d 1124, 1126 (Pa. 1996) ("By virtue of the Supremacy Clause of the United States Constitution, Article VI, Section 2, the Federal Act preempts the ability of the states to adopt legislation that would be less restrictive in allowing interceptions."), *cert. denied*, 518 U.S. 1019 (1996).

31. *See* 18 PA. CONST. STAT. ANN. § 5703; *cf. Wiretap Act*, LAWYERS.COM, http://communications-media.lawyers.com/privacy-law/wiretapping.html [https://perma.cc/EL3J-N67M] (last visited Mar. 28, 2016) (providing detailed summary and legal consequences of federal Wiretap Act).

32. *See, e.g.*, Commonwealth v. Spangler, 809 A.2d 234, 237 (Pa. 2002) (citing Commonwealth v. De Marco, 578 A.2d 942, 949 (Pa. Super. Ct. 1990)) (discussing hesitation to broaden exceptions found under Pennsylvania Wiretap Act). In addressing the issue before it, the Pennsylvania Supreme Court relied on other cases in ensuring that the Pennsylvania Wiretap Act emphasizes the protection of privacy. *See id.*

33. *See* Commonwealth v. Proetto, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) (discussing expectation of privacy on internet), *appeal granted in part by* 790 A.2d 988 (Pa. 2002) (mem.), *and order aff'd by* 837 A.2d 1163 (Pa. 2003) (mem.). The court said,

> While engaging in a conversation over the telephone, a party would have no reason to believe that the other party was taping the conversation. Any reasonably intelligent person, savvy enough to be using the Internet, however, would be aware of the fact that messages are received in a recorded format, by their very nature, and can be downloaded or printed by the party receiving the message. By the very act of sending a communication over the Internet, the party expressly consents to the recording of the message.

Id. In further discussing this issue, the *Proetto* court held that conversations on the Internet, similar to messages left on an answering machine, indicate mutual consent of the parties to recording. *See id.* at 830 (citing Commonwealth v. De Marco, 578 A.2d 942 (Pa. Super. Ct. 1990); *see also* Judge Jessica Brewbaker, *What are Pennsylvania's wiretapping laws? The*

determine whether a possible interception falls under the various exceptions noted in the Pennsylvania Wiretap Act.[34] For example, exceptions to the general requirement to obtain a warrant include when a police officer interacts directly with a suspected criminal or if one party to the conversation consents to an interception.[35] An even greater source of confusion arises when a police officer is not directly involved in the conversation.[36] Pennsylvania courts must resolve the confusion stemming from the Pennsylvania Wiretap Act by balancing law enforcement and privacy interests.[37]

C. *Storage Almost Full: Courts Slow to Find Reasonable Expectation of Privacy in Text Messages*

In reviewing the Fourth Amendment regarding technology, courts have historically been reluctant to find a blanket right to privacy in information.[38] Often, the government will rely on the "misplaced trust" exception to the *Katz* test to argue that an individual has no reasonable expectation of privacy in the

---

Judicial Notice with Judge Jessica Brewbaker, PENNLIVE, http://www.pennlive.com/living/index.ssf/2013/06/the_judicial_notice_the_law_on.html (last visited Mar. 31, 2016) (comparing privacy under Pennsylvania Wiretap Act to Federal Wiretap Act). Some states, including Pennsylvania, also allow for one-party consent to record telephone conversations. *See id.*

34. *See* Commonwealth v. Diego, 119 A.3d 370, 380–81 (Pa. Super. Ct.) (providing court's analysis of whether police actions constituted interception), *appeal denied*, 129 A.3d 1240 (Pa. 2015) (mem.) (unpublished table decision).

35. *See* 18 PA. CONST. STAT. ANN. § 5704(2)(ii)–(iii) (providing exceptions to requirement to obtain warrant for interception). *See generally* Commonwealth v. Cruttenden, 58 A.3d 95, 95–96 (Pa. 2012) (holding officer directly engaging in conversation is not intercepting for purposes of statute); *Proetto*, 771 A.2d at 832 (holding no interception occurred when police officer interacted directly with defendant in online chat room); *see also What are Pennsylvania's wiretapping laws?*, *supra* note 33.

36. *See generally* 18 PA. CONST. STAT. ANN. § 5702 (defining *intercept*); *see also Diego*, 119 A.3d at 380 ("The definition of 'intercept' . . . specifically excludes 'the acquisition of the contents of a communication made through any electronic, mechanical or other device or telephone instrument to an investigative or law enforcement officer . . . .").

37. *See* Karoly v. Mancuso, 65 A.3d 301, 303 (Pa. 2013) (noting that statute prohibits interception of private communications "except pursuant to specified procedures"). In *Karoly*, the court addressed the issue of whether certain conversations made from jail could be accessed without violating the Wiretap Act. *See id.* at 305. The court provided that the Pennsylvania Wiretap Act does "allow county correctional facilities to monitor and record inmate phone calls without any specific prior authorization, so long as inmates are notified in writing and anyone calling into the facility is also told that his call may be monitored and recorded" and these recordings may only be turned over to authorities in order to "safeguard the facility." *See id.* at 303-04 (citing 18 PA. CONST. STAT. § 5704(14) (2015)). However, the court clarified that attorney-client conversations are not subject to interception in order to protect the legal privilege. *See id.* at 304.

38. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 117 (1984) (describing proposition that there is no expectation of privacy when one reveals information to third party). The Supreme Court noted that when one reveals information to a "confidant," there is a chance that person will turn over that information to the government, and the government may use that information without violating the Fourth Amendment. *See id.*; *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (stating that when people reveal bank deposit slips to others, they risk that information being shared with government).

information one relays to others.[39] While some commentators have postulated that the Supreme Court held that individuals have a reasonable expectation of privacy in text messages, the government maintains that lower courts still retain broad power to determine this issue.[40]

Courts exercising broad deferential power to analyze reasonable expectation of privacy issues regarding text messages often rely on reasoning similar to that of the Supreme Court in *United States v. Jacobsen*.[41] In *Jacobsen*, the defendants were arrested after the employees of "a private freight carrier" opened a suspicious package and found a "white powdery substance."[42] The freight carrier then contacted personnel at the Drug Enforcement Administration (DEA) who determined that the substance was cocaine, obtained a warrant, searched the location of the intended recipient, and arrested the defendants.[43] The trial court denied the motion to suppress the evidence, but the court of appeals reversed, holding that testing the substance was an improper expansion of the original search and a warrant was required.[44] In overruling the court of appeals, the Supreme Court discussed the idea that when someone reveals private information to another person, there is a risk that the information will be shared with a third party or law enforcement, and the Fourth Amendment does not prohibit the government from using that information.[45]

---

39. *See, e.g.*, *Jacobsen*, 466 U.S. at 117 (noting that when privacy interest has already been frustrated, authorities can use information without violating Fourth Amendment); *see also* Vitale, *supra* note 18, at 1120 (discussing various exceptions to Fourth Amendment warrant requirement). The misplaced trust doctrine is similar to the "third-party doctrine" enunciated by the *Katz* court. *See id.*

40. *See* City of Ontario v. Quon, 560 U.S. 746, 757 (ruling search of text messages reasonable, "even assuming Quon had a reasonable expectation of privacy"); *see also* Vitale, *supra* note 18, at 1110 ("The [Supreme] Court has given wide deference [] to lower courts in deciding matters pertaining to cell phone privacy."). Vitale argues that the Supreme Court's reluctance in *Quon* to decide "whether a text message sender had Fourth Amendment protections in a context outside of the workplace" indicates the Court may consider reexamining this issue and extend the letter analogy to "mobile communication in the twenty-first century." *See id.* at 1125.

41. 466 U.S. 109, 125-26 (1984) (holding warrantless "seizure" was reasonable when privacy rights had already been infringed "as the result of private conduct").

42. *See id* at 111–12 (discussing private search of shipped packages). During shipment, the package was damaged. *See id.* When examining the damaged package, the freight employees noticed a suspicious substance and notified the DEA. *See id.*

43. *See id.* (discussing search and arrest of defendants). The defendants were indicted for possessing an illegal substance with intent to distribute. *See id.*

44. *See id.* (examining procedure of case). The court of appeals held that the DEA agent's warrant depended "on the validity of the agents' warrantless test of the white powder, that the testing constituted a significant expansion of the earlier private search, and that a warrant was required." *Id.* (footnote omitted).

45. *See id.* at 126 (holding expectation of privacy had "already been frustrated" enough to eliminate constitutional protections); *see also id.* at 115–16 (noting that government action may not "change the nature of the search" such that search becomes "additional search subject to the warrant requirement" (internal quotation marks omitted)). The Supreme Court found that the DEA agent's warrant was valid as the "initial invasions of [the defendants'] package were occasioned by private action." *See id.* at 115. The Court also found that, in order to violate the defendants' Fourth Amendment rights, the subsequent testing of the substance by the DEA had to "exceed the scope of the private search." *See id.*

As technology has developed, courts have struggled to determine whether an expectation of privacy is reasonable.[46] Many courts have compared electronic messages to archaic forms of correspondence, such as written letters.[47] In *Guest v. Leis*,[48] there was an investigation into the use of obscenity on an online computer bulletin board.[49] While the Sixth Circuit ruled for the defendants on other grounds, the court noted that, like a letter, once the message had been delivered to its intended recipient, the sender no longer had a reasonable expectation of privacy in those messages.[50]

Many courts have been reluctant to view text messages as distinct and

---

46. *See, e.g.*, United States v. Jones, 149 Fed. App'x 954, 959–60 (11th Cir. 2005) (analyzing expectation of privacy in text messages and e-mails as matter of first impression). The court cited the subjective and objective prongs from *Katz* to determine whether a reasonable expectation of privacy exists. *Id.* However, the court also pointed out the existence of the third party exception. *See id.* The court further likened text messages to e-mail messages, finding, "[t]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny." *Id.* at 959 (quoting United States v. Maxwell, 45 M.J. 406, 418 (U.S.A.F. 1996)) (internal quotation marks omitted).

47. *See id.* ("Those circuits that have addressed the question have compared e-mails with letters sent by postal mail."); *see also* Vitale, *supra* note 18, at 1123–24 (discussing difficulty with analogizing text messages to letters). Vitale argues that the letter analogy is "insufficient and logically inconsistent." *See id.* (quoting Katharine M. O'Connor, Note, *:o OMG They Searched My Txts: Unraveling the Search and Seizure of Text Messages*, 2010 U. ILL. L. REV. 685, 686) (internal quotation marks omitted).

> First, text messages are transmitted in a matter of seconds, while letters are delivered in a matter of days. Consequently, "any reasonable expectation of privacy that existed is obliterated just as quickly as the message is delivered." . . . Finally, as technology evolves, courts should consider not only the sophistication of the technology but also the way in which people relate to and interact with the technology.

Id. (footnotes omitted). Even though courts have analogized text messages and letters, letter senders have some privacies that are not enjoyed by text message senders, such as the law making it a federal offense to open a letter addressed to someone else. *See id.* at 1124–25.

48. 255 F.3d 325 (6th Cir. 2001).

49. *See id.* at 330-32 (discussing facts of case). The system in which the obscenities were found included "thousands of subscribers from the Greater Cincinnati area, the United States and even overseas." *See id.* at 330 (internal quotation marks omitted). Users of the site could send e-mails to other subscribers as well as participate in "chat room conversations, on-line games, and conferences." *See id.* Officers from the Hamilton County, Ohio, Regional Electronic Computer Intelligence Task Force (RECI) often would download obscene images and present them to a court in order to obtain a warrant. *See id.* The offenses in question included pandering obscenity, which violated an Ohio statute. *See id.* When the officers executed the warrant, they were unable to obtain just the obscene images from the computer, so they dismantled the computer and removed it from the house. *See id.* at 330–31. One of the issues the court decided was whether this action exceeded the scope of the warrant. *See id.* at 332.

50. *See id.* at 333 (citing United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995)) (analogizing e-mailers to letter-writers). "They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter." *Id.* (quoting *King*, 55 F.3d at 1196).

continue to analogize them to older means of communication.[51] However, in *State v. Patino*,[52] the Rhode Island Supreme Court focused specifically on the issue of privacy in text messages as an issue of first impression for Rhode Island.[53] The most common context in which this question arises occurs when law enforcement search a suspect's own cell phone incident to arrest.[54] In *Patino*, however, the court reviewed the issue of whether text messages stored in another's phone are subject to a reasonable expectation of privacy.[55] The defendant was indicted for first-degree murder of his girlfriend's six-year old son; the prosecution was mostly premised on incriminating text messages sent by the defendant and discovered on his girlfriend's cell phone.[56]

In analyzing whether the evidence obtained should have been suppressed for illegal search and seizure, the court looked to approaches taken by other jurisdictions to determine whether one has a reasonable expectation of privacy in text messages stored in another's phone.[57] While the court acknowledged

51. *See* State v. Patino, 93 A.3d 40, 54 (R.I. 2014) (noting hesitancy to adapt to new technology, stating "[i]t is often not easy to pour new wine into old wineskins, yet wise stewardship might suggest the use of the old skins until they burst"), *cert. denied*, 135 S. Ct. 947 (2015) (mem.); *see also Jones*, 149 Fed. App'x at 959 (noting defendant had no reasonable expectation of privacy in text messages stored in another's phone). The *Jones* court discussed Justice Harlan's concurrence in *Katz*. *See id.* By analogizing text messages to letters and e-mails, in which privacy interests erode upon delivery, the court grouped text messages with other forms of technology, and accepted those cases as precedent. *See id.*

52. 93 A.3d 40 (R.I. 2014), *cert. denied*, 135 S. Ct. 947 (2015) (mem.).

53. *See id.* at 55 (noting issue is of first impression).

54. *See generally* Sara M. Corradi, Comment, *Be Reasonable! Limit Warrantless Smart Phone Searches to* Gant*'s Justification for Searches Incident to Arrest*, 63 CASE W. RES. L. REV. 943, 944–54 (2013) (examining standard for lawful search of smart phones incident to arrest). The author analyzes lower courts' analyses of warrantless cellphone searches. *See id.* at 948–52. Corradi refers to a Fifth Circuit decision that compared a cell phone to a closed container that may be searched incident to arrest. *See id.* at 948. She also discusses a Fourth Circuit decision that held that, incident to arrest, text messages may be searched without a warrant and recorded in order to preserve the information in *United States v. Young*. *See id.* at 949.

55. *See Patino*, 93 A.3d at 54–58 (discussing issue in case).

56. *See id.* at 42 (summarizing facts of case). While investigating the crime scene, the police officer searched a cell phone after it received a text message. *See id.* at 44–45. He noticed the phone on the counter and one "indicated audibly and by light that it was receiving a message." *Id.* at 44 (internal quotation marks omitted). The police officer picked up the phone to see if it was the victim's father or someone else calling to inquire about the victim's condition. *See id.* Seeing there was a new message, the officer "'manipulated the button' on the phone, which led to a mailbox listing incoming and outgoing text messages. [The officer] testified that, upon seeing the word 'hospital' in a text message," he opened the folder and read a message that referred to the child's injuries. *Id.* The officer testified that he did not read any more messages, but he did relay the information from that message to another officer. *See id.* At one point, the officer noticed that a phone was missing, and contacted headquarters notifying them that, "[t]here is possibly some information that needs to be protected on it . . . ." *See id.* (first alteration in original) (internal quotation marks omitted). Another officer was able to obtain a warrant, which allowed the officers to find further text messages that ultimately incriminated the defendant. *See id.* at 44–45.

57. *See id.* at 52–53 (discussing how U.S. Supreme Court has determined reasonableness for other cases). The *Patino* court cited to a Supreme Court concurrence, which pointed out that "'[T]echnology can change those expectations [of privacy]. Dramatic technological change may lead to periods in which popular expectations are in flux and may

that advances in technology could lead to different results, its analysis ultimately turned on whether the defendant owned or was the primary user of the cell phone.[58] The court determined that the location of the seized text messages is the most important factor in finding an expectation of privacy and that the sender loses control over the messages once they are sent.[59]

D. *Software Update Available: Courts Adjust to New Technology and Find Reasonable Expectation of Privacy in Text Messages*

In recent years, with the continued emergence of new technology, some courts have recognized the need to modify the old rules, particularly regarding text messages.[60] In *City of Ontario v. Quon*,[61] the United States Supreme Court had the opportunity to determine whether text messages stored in another's device were subject to a reasonable expectation of privacy, but the Court did not

---

ultimately produce significant changes in popular attitudes.'" *Id.* at 52 (alterations in original) (quoting United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring)). Further, the Supreme Court has acknowledged that "'[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior[.]'" *Id.* at 52–53 (alteration in original) (quoting City of Ontario v. Quon, 560 U.S. 746, 748 (2010)); *see also id.* at 55 (noting that courts have often compared text messages to other forms of communication, such as personal computers, e-mails, address books and laptops).

58. *See id.* at 55. The Fifth Circuit in *Finley* held that "the defendant had a reasonable expectation of privacy in [the defendant's] cell phone because . . . he 'maintained a property interest in the phone, [and] had a right to exclude others from using the phone[.]'" *Id.* (third alteration in original) (quoting United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007)).

59. *See id.* at 55–56 (noting that "idea of control has been central" to court's determinations under Fourth Amendment). The *Patino* court also noted that the United States Supreme Court considered control as a factor in reviewing the expectation of privacy in an item when determining the "distinction 'between the Fourth Amendment rights of passengers and the rights of an individual who has *exclusive control* of an automobile" in *Rakas v. Illinois*. *See id.* at 56 (quoting Rakas v. Illinois, 439 U.S. 128, 154 (1978)). For other cases considering control as a factor, see United States v. Davis, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011) (noting reasonable expectation of privacy in contents of one's own phone); State v. Boyd, 992 A.2d 1071, 1081 (Conn. 2010) (finding reasonable expectation of privacy over phone because it would have been reasonable for trial court to conclude defendant "exercised exclusive control over it"); State v. Bone, 107 So. 3d 49, 66 (La. Ct. App. 2012) (finding reasonable expectation of privacy when one "ha[s] a possessory interest in the phone as the exclusive user").

60. *See, e.g.*, United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) ("[A]nalogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life."); *see also* Corradi, *supra* note 54, at 958–59 (noting that courts have found that "computers have a heightened expectation of privacy and require police to obtain a specific warrant for the computer prior to searching its contents"); Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165, 1200–01 (2008) (arguing that cell phones are comparable to computers). Stillwagon argues that, because cell phones have the ability to contain as much information as a computer, cellphones should be classified as computers. *See* Stillwagon, *supra*, at 1201. The author bases this argument on the possibility that "a look into a cell phone's memory can reveal a subjective picture of our life." *Id.* (internal quotation marks omitted).

61. 560 U.S. 746 (2010).

rule on that issue.[62] In *Quon*, an employee's government-provided pager was searched after he violated the terms of use by sending and receiving too many messages.[63] While the Supreme Court did not address whether an individual has a reasonable expectation of privacy in text messages stored on another person's device, the Court determined that the defendant had a reasonable expectation of privacy in messages sent from his pager.[64] In finding for the City, the Supreme Court held that although there was an expectation of privacy in the text messages, the City's search was nonetheless reasonable because it fell under the "special needs of the workplace" exception.[65] Further, in dicta, the Court acknowledged that "cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[66]

In recent years, courts have sought to expand the Fourth Amendment to keep pace with changing technology.[67] The Supreme Court recently decided such an issue in *Riley v. California*.[68] In *Riley*, police obtained data stored on a drive-by shooting suspect's cell phone without a warrant.[69] The defendant moved to suppress the evidence against him, and the Supreme Court held that the police generally may not search a cell phone seized from an individual upon arrest without first obtaining a warrant.[70] The Court noted that "[m]odern cell phones are not just another technological convenience. . . . [T]hey hold for

62. *See id.* at 765 (noting it is not necessary to decide issue in this case).

63. *See id.* at 750–52 (discussing facts of case). The City of Ontario Police Department provided pagers to its employees. *See id.* at 750–51. In using the pagers, the employees had to abide by a "Computer Usage, Internet and E–Mail Policy" which gave the City "the right to monitor and log all network activity including e-mail and Internet use." *Id.* at 751 (internal quotation marks omitted). When Quon exceeded his limit multiple times, his superior audited his messages and revealed most messages were not related to work. *See id.* at 751–53.

64. *See id.* at 760 (assuming Quon had reasonable expectation of privacy in messages sent by him on his pager).

65. *See id.* at 760–61 (quoting O'Connor v. Ortega, 480 U.S. 709, 725 (1987) (plurality opinion)) (internal quotation marks omitted) (noting "the 'special needs' of the workplace" trumps unreasonable warrantless searches). The Court found that "clearly communicated" employer policies can "shape" employees' reasonable expectations. *See id.* at 760.

66. *See id.* at 760 (noting that pervasiveness of cell phones may "strengthen" case for expectation of privacy); *see also* Vitale, *supra* note 18, at 1110 n.3 (noting courts have relied on this language to find broad expectation of privacy).

67. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."); *see also* Soma et al., *supra* note 21, at 526–28 (discussing legal approaches to privacy issue). Soma and his co-authors argue that "[t]he right to privacy should not be limited to any particular medium or form of expression." *Id.* at 526 (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205–06 (1890)) (internal quotation marks omitted).

68. 134 S. Ct. 2473, 2484 (2014) ("These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones . . . .").

69. *See id.* at 2480–81 (discussing facts of case). Incident to arrest, police seized a cell phone from the subject and searched its contents, finding photographs and videos that proved the defendant was involved in a gang. *See id.*

70. *See id.* at 2485 (holding that warrants are required to search "data on cell phones").

many Americans 'the privacies of life.'"[71]

The Washington State Supreme Court recently addressed this expansive view of cell phone privacy in *State v. Hinton*.[72] In *Hinton*, a detective arrested a man for possession of heroin and seized his cell phone in the process.[73] The detective then responded to an incoming text message on the man's cell phone and set up a drug deal.[74] The detective subsequently arrested the defendant.[75] The court ruled for the defendant and found that the text message conversation was private and that the detective was required to obtain a warrant before seizing such information.[76] Despite no longer having physical control over his text messages, the court thought the defendant was still entitled to a reasonable expectation of privacy in the messages he sent.[77] The Washington Supreme Court recognized the need to respond to the emergence of new technology and acknowledged that, while legislatures and courts must strike a balance between fighting crime and privacy, ease of communication should not erode privacy interests.[78]

III. PENNSYLVANIA SUPERIOR COURT REJECTS CALL TO UPDATE PRIVACY ISSUES IN *COMMONWEALTH V. DIEGO*

In *Commonwealth v. Diego*, the Pennsylvania Superior Court refused to consider modern uses of technology in deciding that individuals do not have a reasonable expectation of privacy in sending a text message.[79] The court read the text of the Pennsylvania Wiretap Act narrowly and held that no interception had occurred.[80] In reaching its holding, the court avoided a deeper discussion of the expectation of privacy in text messages and the loophole in the

71. *See id.* at 2494–95 (citation omitted) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)) (noting that before seizing cell phone police should get warrant).

72. 319 P.3d 9, 16 (Wash. 2014) (en banc) (acknowledging increased use of text messages to discuss private matters).

73. *See id.* at 11 (discussing facts of case). The court analyzed "whether a text message conversation was 'a private affair[]' protected from a warrantless search" under the Washington Constitution. *Id.* (alteration in original).

74. *See id.* (discussing facts).

75. *See id.* (discussing facts).

76. *See id.* (noting holding of case). The Washington Supreme Court looked to the state's historical treatment of phone calls and other electronic communications to determine that text messages are subject to an expectation of privacy. *See id.* at 14.

77. *See id.* at 14–15 (rejecting notion that control determines whether messages are private). The Washington Supreme Court decided this case based on its state constitution, rather than the Fourth Amendment. *See id.* ("Given the realities of modern life, the mere fact that an individual shares information with another party and does not control the area from which that information is accessed does not place it outside the realm of [the Washington Constitution's] protection.").

78. *See id.* at 14 (acknowledging that Washington law favors privacy over needs of law enforcement); *see also* Soma et al., *supra* note 21, at 504 (discussing growing expectation of privacy in e-messaging).

79. For a thorough discussion of the *Diego* decision regarding a reasonable expectation of privacy, see *infra* notes 96–112 and accompanying text.

80. For a discussion of the superior court's reasoning regarding the Pennsylvania Wiretap Act, see *infra* notes 113–25 and accompanying text.

Pennsylvania Wiretap Act.[81]

A. *Siri, Please Tell Me the Facts of* Commonwealth v. Diego

After determining that Mr. Gary Still had been involved in a firearms theft, Detective James Moyer (the detective) apprehended Still at Still's father's residence.[82] The detective read Still his *Miranda* rights, and Still soon admitted to stealing the firearms, which he later used to trade for heroin.[83] After learning this, the detective asked Still to set up a heroin deal, and police officers told him "it would be in his best interest to do so."[84] Still agreed and explained that he would "use the text messaging service on his iPad" to communicate with Diego.[85] During the transaction, Still texted Diego from his iPad and relayed each message to the detectives.[86] Still scheduled the transaction to take place at a local hotel, and police officers were able to arrest Diego.[87]

Following his arrest, Diego filed a motion to suppress the evidence used

---

81. For a discussion of the superior court's rejection of the Appellant's Brief, see *infra* notes 116–25 and accompanying text.

82. *See* Commonwealth v. Diego, 119 A.3d 370, 372–73 (Pa. Super. Ct. 2015) (describing police investigation of Mr. Gary Still), *appeal denied*, 129 A.3d 1240 (Pa. 2015) (mem.) (unpublished table decision). According to the factual summary of the trial court, the detective "determined that Mr. Still was involved in the theft of approximately twelve (12) firearms from the residence . . . ." *Id.*

83. *See id.* (describing Still's confessions). Still admitted to stealing numerous guns over eight weeks, two of which he exchanged for heroin with Diego. *See id.* Still organized the transactions with his iPad, which the police previously confiscated during the firearms negotiation. *See id.*

84. *See id.*

85. *See id.*

86. *See id.* (describing Still's transaction with Diego). Still sat with at least six detectives in the basement of the police station and relayed each response from Diego to the detectives. *See id.* Detective Moyer testified that an officer was sitting next to Still and "it was possible that the officer observed what Mr. Still was doing on the iPad." *See id.* at 372–73. The trial court found that:

> "[d]uring the communication, officers were in the room contemporaneously observing and directing, but *not themselves* doing the communicating. . . . The officers['] giving direction to Still, and watching over him, amounts to eavesdropping or listening in on the electronic message communication." The court also noted that "it was [Still] who initiated the phone call at the direction of the officers; the clear intent was to intercept."

Id. at 381 n.2 (alterations in original) (citation omitted) (quoting Commonwealth v. Diego, No. 22–CR–0001203–2013 (C.P. Dauphin Mar. 16, 2015)). While the suppression court relied on this information to suppress the evidence obtained, the detective rejected this description of the facts:

> We asked Mr. Still if he would be willing to set up a deal with his dealer that evening, which he agreed to do. From that point, he said he usually contacts [Appellee] with an i[P]ad through a text messaging service on his i[P]ad. He was provided his i[P]ad. He then set up the deal. He asked what he should do. I said, [j]ust do your deal the way you normally would. He set it up. *He relayed to me what was going on*. The deal was set up.

Id. (alterations in original) (quoting Transcript of Proceedings, Suppression Hearing - Vol. 1, at 7, Commonwealth v. Diego (C.P. Dauphin Jan. 31, 2014), No. 22–CR–0001203–2013).

87. *See id.* at 373 (describing transaction and Diego's subsequent arrest).

against him.[88] At the hearing, "the trial court requested that the parties brief the suppression-related issues[,]" and on October 28, 2014, the court granted Diego's suppression motion.[89] Consequently, the Commonwealth appealed to the Superior Court of Pennsylvania.[90]

B. *Renewing Two-Year Contract: The Superior Court Maintains the Status Quo in Its* Diego *Analysis*

In holding for the Commonwealth, the Pennsylvania Superior Court addressed three separate issues, eventually overturning the trial court opinion and finding that the text messages need not be suppressed.[91] The court held that the appellee's iPad was not a "device" as defined in the Pennsylvania Wiretap Act, that Diego lacked a reasonable expectation of privacy in his text message communications, and that the trial court erred in granting Diego's motion to suppress evidence because Diego's text messages were not "intercepted" in violation of the Pennsylvania Wiretap Act.[92]

1. *A New Model: An iPad Is Not a Device*

The court first discussed whether Diego's iPad fell under the Pennsylvania Wiretap Act's definition of *device*.[93] Under the Pennsylvania Wiretap Act, using what courts have termed the "telephone exemption," a police officer may use a telephone in the "ordinary course of his duties" to intercept a wire, electronic, or oral communication.[94] The court held that an iPad was an "electronic, mechanical, or other device" and therefore did not fall under the telephone exemption of the Pennsylvania Wiretap Act.[95]

---

88. *See id.* (explaining Diego's motion to suppress evidence). Diego argued that "[t]he police supervised and observed the text-message conversation between Still and his drug supplier as it was occurring on the iPad." *See id.* at 381 n.2 (alteration in original) (quoting Brief for Appellee at 3, Commonwealth v. Diego, 110 A.3d 370 (Pa. Super. Ct. 2015) (No. 1989 MDA 2014) [hereinafter Brief for Appellee], 2015 WL 5666844, at *3).

89. *See id.* at 373 (providing lower court's holding).

90. *See id.* (referring to Commonwealth's timely appeal).

91. *See id.* at 373 (indicating three issues to address on appeal and holding of court).

92. *See id.* at 375–76 (describing superior court's holding).

93. *See id.* at 374 (framing issue).

94. *See id.* (citing 18 PA. STAT. § 5702 (1973)) (discussing telephone exemption under Pennsylvania Wiretap Act). The Commonwealth argued that an iPad should fall under the telephone exemption to the Pennsylvania Wiretap Act. *See id.* The Commonwealth sought to rely on this exception by arguing that the iPad "was being used as the functional equivalent of a modern cellular phone . . . ." *See id.*

95. *See id.* (holding iPad cannot be classified as telephone and therefore cannot be used to intercept messages under telephone exemption to Pennsylvania Wiretap Act). The superior court rejected the Commonwealth's argument and refused to expand the definition of device under the Pennsylvania Wiretap Act to include an iPad. *See id.* The court stated that Diego's iPad was not a device under the statute because it was not used to intercept a communication, there was no evidence that Diego even used an iPad to communicate with Still, and Still's iPad was the "origin of the intercepted message, and not the device that purportedly intercepted that message." *See id.* Further, the court rejected the Commonwealth's argument that the Supreme Court of Pennsylvania broadened the telephone exemption in *Commonwealth v. Spence*, 91 A.3d 44 (Pa. 2014). *See id.* at 375. In *Spence*, a police officer

2. *What's Your Password? Court Finds No Reasonable Expectation of Privacy in Sent Text Messages*

Second, the superior court addressed whether one has "a reasonable expectation of privacy in the contents of [a] text message conversation . . . ."[96] The court heavily relied on the earlier decision of *Commonwealth v. Proetto*,[97] which considered the expectation of privacy in chat room conversations.[98] In *Proetto*, the court held that one "savvy enough to be using the Internet" should be aware that the messages sent could be downloaded and shared, and in sending such a message, that person "expressly consents to the recording of the message."[99] Relying on *Proetto*, the Commonwealth argued that Diego "lacked a reasonable expectation of privacy" in his text message conversation.[100] Diego disagreed with this argument and sought to distinguish text messages from chat room conversations.[101] In his brief, Diego explained that in a chat room conversation, neither the sender nor any recipient of the messages can delete the message once it is posted.[102] He contrasted this by noting that the recipient of a

instructed an informant to make a phone call and turn on the speakerphone to allow the officer to listen to the conversation. *See id.* While the defendant argued that the "phone was not a phone under the Act with respect to the trooper" because the officer was not a subscriber to that specific phone's service plan, the court rejected this argument and held that the language of the statute specifically exempts telephones from the definition of *device*, and does not consider how the telephone is used. *See id.* (citing *Spence*, 91 A.3d at 47). In the present case, the superior court held that an iPad is not a telephone under the "common understanding of the relevant terms" and "[t]he fact that an iPad or any other tablet computer can perform functions similar or identical to a modern cellular phone is not dispositive . . . ." *See id.* Finally, the court also held it does not possess the power to broaden the interpretation of the term "telephone" under the Pennsylvania Wiretap Act. *See id.* at 375–76.

96. *See id.* at 376 (stating second issue of case).

97. 771 A.2d 823 (Pa. Super. Ct. 2001), *appeal granted in part by* 790 A.2d 988 (Pa. 2002) (mem.), *and order aff'd by* 837 A.2d 1163 (Pa. 2003) (mem.).

98. *See Diego*, 119 A.3d at 376 (quoting *Proetto*, 771 A.2d at 829) (discussing expectation of privacy in e-mail or chat room conversations).

99. *See id.* at 376–77 (citing *Proetto*, 771 A.2d at 829) (finding lack of expectation of privacy in Internet communications). In *Proetto*, the court first discussed the expectation of privacy in telephone conversations and determined that while a person is engaging in a telephone conversation, that person "would have no reason to believe that the other party was taping the conversation." *See id.* at 376 (quoting *Proetto*, 771 A.2d at 829). It then likened sending an e-mail or chat room message to leaving a message on an answering machine. *See id.* at 376–77 (quoting *Proetto*, 771 A.2d at 830).

> The sender knows that by the nature of sending the communication a record of the communication, including the substance of the communication, is made and can be downloaded, printed, saved, or, in some cases, if not deleted by the receiver, will remain on the receiver's system. Accordingly, by the act of forwarding an e-mail or communication via the Internet, the sender expressly consents by conduct to the recording of the message.

Id. (quoting *Proetto*, 771 A.2d at 830).

100. *See id.* (presenting Commonwealth's argument).

101. *See id.* at 377 (quoting Brief for Appellee, *supra* note 88, at 9–10) (arguing that text message conversations and chat room conversations are inherently different).

102. *See id.* (asserting that chat room messages are not private because they cannot be deleted and once sent, "the proverbial bell cannot be unrung" (quoting Brief for Appellee, *supra* note 88, at 9-10)).

text message can delete it, and the recipient of a text message is often a single individual.[103] Diego argued that these differences were dispositive, that a text message should be distinguished from an Internet chat room message, and that the *Proetto* decision should not apply.[104] Additionally, Diego relied on the Supreme Court's *Riley* decision that held police may not search a smart phone incident to arrest without obtaining a search warrant.[105]

The *Diego* court rejected Diego's argument and instead invoked *Proetto*, noting that *Proetto* applied to both e-mails and chat room posts.[106] The court compared text messages to e-mails, saying that e-mails and text messages both can be deleted by the recipient and both are often sent to only one recipient.[107] The court also held that under the "mutual consent provision" of the Pennsylvania Wiretap Act, Diego should have known that his message was being recorded and could be shared.[108] The court reasoned that because the sender of a text message has knowledge that the message will be recorded, the sender loses any reasonable expectation of privacy once that message is sent.[109]

Further, the court rejected Diego's reliance on *Riley* and found the heightened expectation of privacy in text messages was not relevant to the facts at bar.[110] Unlike in *Riley*, the police in *Diego* did not search Diego's phone incident to arrest, so the heightened expectation of privacy was not applicable.[111] The court concluded its analysis of the expectation of privacy issue by comparing text messages to e-mails and first-class mail, holding "[w]hen an individual sends a text message, he or she should know that the

---

103. *See id.* (quoting Brief for Appellee, *supra* note 88, at 9-10) (contrasting chat room conversations and text message conversations). Diego also argued that an Internet chat room is "potentially populated by boundless, anonymous individuals," and therefore chat room discussions are inherently different from text messages. *See id.* (quoting Brief for Appellee, *supra* note 88, at 9-10).

104. *See id.* (quoting Brief for Appellee, *supra* note 88, at 9-10) (distinguishing text message from chat room post).

105. *See id.* at 377–78 (invoking Supreme Court decision in *Riley v. California*). Diego argued that *Riley* granted a "heightened expectation of privacy" in cell phone usage. *See id.* at 377.

106. *See id.* (referring to superior court's inclusion of e-mails in its analysis in *Proetto*).

107. *See id.* (finding that text messages and e-mails are substantially similar).

108. *See id.* (citing Commonwealth v. De Marco, 578 A.2d 942, 948 (Pa. Super. Ct. 1990)) (discussing why "answering machine tapes fall within the mutual consent provision of the Wiretap Act"). The *De Marco* court held that a "reasonably intelligent person" leaving a message on an answering machine "would have to be aware of, and *consented by conduct to*, the recording of the message on the answering machine tape." *Id.* (quoting *De Marco*, 578 A.2d at 948).

109. *See id.* (rejecting differences between chat rooms, e-mails, and text messages). The court held that the idea of control and the "ability to delete" messages are irrelevant. *See id.* (internal quotation marks omitted). Rather, "[i]t is the sender's knowledge that the communication will automatically be recorded, surmised from the very nature of the selected means of transmission, that is dispositive of the sender's lack of an expectation of privacy or, at least, the lack of any reasonable expectation of privacy." *Id.* (quoting *De Marco*, 578 A.2d at 948).

110. *See id.* at 378 (rejecting Diego's reliance on *Riley*).

111. *See id.* (distinguishing facts in *Diego* from those in *Riley*).

recipient, and not the sender, controls the destiny of the content of that message once it is received."[112]

3. *Text Delivered: Wiretapping and Electronic Surveillance Control Act*

Finally, the court addressed the issue of whether an "interception" within the statutory definition of the Pennsylvania Wiretap Act occurred.[113] The Commonwealth relied on two cases in which the courts determined, because the law enforcement officers were direct parties to conversations, no interception had occurred.[114] Because there was "less police intrusion" in *Diego* than in those two cases, the Commonwealth argued that no interception occurred.[115]

The superior court rejected the Commonwealth's argument because the Pennsylvania Wiretap Act specifically exempts law enforcement officers who communicate directly with a suspected defendant from violating the Act.[116] This did not occur in *Diego*, as the police officers were communicating with an informant, and not directly with Diego, so the holdings from those cases did not apply in *Diego*.[117] Additionally, the court rebuked the Commonwealth for not providing "support for the proposition that what is or is not an intercept under the Wiretap Act turns on the magnitude of the 'police intrusion.'"[118]

The court nonetheless concluded that no interception occurred in the case.[119] The court found that Still spoke directly with Diego, and "voluntarily"

112. *See id.* (equating text message conversations to "first-class mail" (quoting *Commonwealth v. Proetto*, 771 A.2d 823, 831 (Pa. Super. Ct. 2001)). The *Proetto* court stated that a sender of a letter "can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause," but once the intended recipient receives and opens the letter, there is no longer an expectation of privacy. *See id.*

113. *See id.* at 379 (explaining that evidence may be suppressed for violations of Pennsylvania Wiretap Act). In an earlier case, the superior court declared that even if an interception does not violate one's reasonable expectation of privacy, law enforcement can still violate the Pennsylvania Wiretap Act by intercepting certain communications. *See id.* (citing Commonwealth v. Deck, 954 A.2d 603, 608–09 (Pa. Super. Ct. 2008)).

114. *See id.* at 379–80 (presenting facts of two cases where evidence was not suppressed). The Commonwealth relied on a case where the Pennsylvania Supreme Court held that when a law enforcement officer "communicates directly with a suspect via cell phone text messages while pretending to be the suspect's accomplice[,]" no interception occurs. *Id.* at 380 (alteration in original) (quoting Commonwealth v. Cruttenden, 58 A.3d 95, 96 (Pa. 2012)). Additionally, the Commonwealth relied on *Proetto*, in which an officer posed as an underage female in a chat room and communicated directly with the defendant. *See id.* (citing *Proetto*, 771 A.2d at 832).

115. *See id.* at 380 (presenting Commonwealth's argument that no interception occurred).

116. *See id.* (discussing exemption for law enforcement officer communicating directly with defendant).

117. *See id.* (rejecting Commonwealth's reliance on *Proetto* and *Cruttenden*). Because no law enforcement officer directly communicated with Diego in setting up a drug transaction, the exemption did not apply. *See id.*

118. *See id.* (noting that no statute or relevant case law references police intrusion as important to decision).

119. *See id.* (holding no interception occurred in violation of Pennsylvania Wiretap Act).

turned over the text messages to the police.[120] The court held that no interception occurred because once a message is received, the communication has ended, and the Pennsylvania Wiretap Act does not govern any longer.[121] The court found relaying text messages to police after receiving them does not "render either his or the police's conduct an 'interception' . . . ."[122]

The court concluded its analysis by determining that an interception must occur "during the transmission of the message, or at least simultaneous to the receipt of the message," which had not happened in *Diego*.[123] While the court acknowledged the situation might have been different had the police read the text messages on Still's iPad as he received them, the court concluded that was not the case and thus did not rule on the matter.[124] The superior court held the trial court erred in suppressing the evidence because there was no constitutional violation of Diego's right to privacy, and the Pennsylvania Wiretap Act did not apply to the circumstances.[125]

IV. UPGRADE YOUR PLAN: *DIEGO* DEMONSTRATES THE NEED FOR A CLOSER LOOK AT PRIVACY ISSUES AND LEGISLATION TO PROTECT AGAINST INTRUSIVE WIRETAPS

In *Diego*, the Pennsylvania Superior Court joined a long list of courts that have refused to adapt to new technology and broaden individuals' expectation of privacy.[126] Pennsylvania courts have similarly refused to find an expectation

120. *See id.* at 380–81 (noting Still, and not police, was party to conversation).

121. *See id.* at 381 (declaring that once message is received, no interception can occur). The court decided that, because Still "was a party to the conversation . . . he could not be said to have intercepted [the message] simply because he received it." *Id.* at 380–81.

122. *See id.* at 381 (interpreting Pennsylvania Wiretap Act). The court further opined that

> [o]nce an individual text message is received by the intended recipient, the communication has ended. Once the communication had ended, it is simply illogical to conclude that subsequent actions constitute intercepts within the meaning of the Wiretap Act. . . . It would be absurd to conclude that anytime an iPad or similar device records a text message conversation that a Wiretap Act violation occurs—for that is the equivalent of saying that everyone receiving a text message on such a device has committed a Wiretap Act violation.

Id.

123. *See id.* (holding no interception occurred).

124. *See id.* at 381–82 (noting that different facts may have led to different opinion). The court noted that the record did not support Diego's "assertion that the police were watching Still's iPad screen over his shoulder as the text messages were sent back and forth to Appellee" but noted that if the police had observed the messages, "a different legal question" would have to be decided "because it would then be plausible to argue that the police may have observed the content of the text messages before Still had received them." *See id.*

125. *See id.* at 382 (reversing suppression order and remanding case).

126. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 126 (1984) (holding when one reveals private information to another, that person assumes risks that information may be shared with third party); United States v. Jones, 149 Fed. App'x 954, 959–60 (11th Cir. 2005) (holding individual sending e-mail loses legitimate expectation of privacy after e-mail is received by other party); State v. Patino, 93 A.3d 40, 57 (R.I. 2014) (holding sender of text messages does not have reasonable expectation of privacy in text messages stored in cellular

of privacy in electronic messages.[127] Analyzing cases similar to *Diego*, Pennsylvania courts should adopt an approach similar to that taken by the Washington State Supreme Court in *Hinton*.[128] Further, Pennsylvania courts should broadly interpret the most recent United States Supreme Court decisions in *Quon* and *Riley* to protect more defendants in cases like *Diego* and find a reasonable expectation of privacy in sent text messages.[129] With the emergence of new technology and the nearly universal use of texting, one should enjoy a reasonable expectation of privacy when sending a text message.[130]

Further, legislation may be necessary to address the loophole in the Pennsylvania Wiretap Act, which allowed the law enforcement officers to direct an informant to relay text messages from a suspected defendant without first obtaining a court-ordered warrant.[131] While providing law enforcement with the tools to combat crime, the Pennsylvania legislature must uphold the privacy rights of citizens of the Commonwealth.[132]

---

telephone belonging to recipient of text messages), *cert. denied*, 135 S. Ct. 947 (2015) (mem.).

127. *See*, *e.g.*, Commonwealth v. Proetto, 771 A.2d 832 (Pa. Super. Ct. 2001) (holding sender of e-mail or chat room messages has no expectation of privacy upon delivery to recipient); Commonwealth v. De Marco, 578 A.2d 942 (Pa. Super. Ct. 1990) (holding person leaving message on answering machine has no expectation of privacy in that message).

128. 319 P.3d 9, 13 (Wash. 2014) (en banc) (holding police detective's conduct in reading text messages and responding invaded defendant's "private affairs").

129. *See* Riley v. California, 134 S. Ct. 2473 (2014) (recognizing heightened expectation of privacy in text messages); City of Ontario v. Quon, 560 U.S. 746 (2010) (noting it was assumed defendant had reasonable expectation of privacy in pager messages).

130. *See* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) (discussing importance of Fourth Amendment keeping pace with technology); *see also* Soma et al., *supra* note 21, at 525–26 (arguing telephone privacy protections should be extended to e-messaging). Soma and his co-authors note that many courts have shown a willingness to find a reasonable expectation of privacy in technology. *See* Soma et al., *supra* note 21, at 526 (describing courts' feelings toward finding privacy expectation for technology). They argue, "'[T]he Fourth Amendment protects people, not places.' In today's world of cyberspace communications, people must be identified with the various e-messaging communication mechanisms they use." *Id.* (alteration in original) (footnote omitted) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)). They also argue Congress "intended . . . to extend telephone privacy protections to other e-messaging forms, but the lack of clarity and exceptions in that statute, along with varying interpretations by the courts, call for a return to basic principles." *See id.* (footnote omitted); *see also* Vitale, *supra* note 18, at 1137–38 (discussing why text messages should be subject to expectation of privacy). Vitale discusses the expectation of privacy opined by the *Katz* doctrine and notes that the Supreme Court "appears to have eliminated the subjective component of the *Katz* test." *See id.* at 1136 (quoting Christopher R. Jones, *"EyePhones": A Fourth Amendment Inquiry into Mobile Iris Scanning*, 63 S.C. L. REV. 925, 935 (2012)) (internal quotation marks omitted). Therefore, Vitale looks solely at whether the expectation of privacy over sent text messages is "shared by society" and determines that, based on studies, "people consider their cell phones to be at least as private of a device as a computer, if not more so." *See id.* at 1136–37.

131. *See* Commonwealth v. Diego, 119 A.3d 370, 381–82 (Pa. Super. Ct. 2015) (noting outcome may have been different if officers observed messages over informant's shoulder), *appeal denied*, 129 A.3d 1240 (Pa. 2015) (mem.) (unpublished table decision); *see also* Nelson, *supra* note 22 (discussing fact that situation could have been different with "one officer glanc[ing] at the iPad screen").

132. *See* Commonwealth v. Spangler, 809 A.2d 234, 236 (Pa. 2002) (noting Wiretap Act emphasizes privacy and provisions are "strictly construed"); *see also* State v. Hinton, 319

A. *Pennsylvania Courts Must Issue New Privacy Policy and Disclosure Statement Relating to Text Messages*

In analyzing whether individuals have a reasonable expectation of privacy in sent text messages, the Pennsylvania Superior Court failed to distinguish text messages from other forms of communication.[133] Holding that the sender of a text message (or chat room message or e-mail) knows the message will automatically be recorded fails to take into account the abundance of personal information shared via these recorded forms of communication.[134]

In recent years, many have noted that it is necessary for future courts to address the modern realities of privacy situations and begin to grant a greater expectation of privacy.[135] Rather than trying to analogize text messages with older means of communication for privacy analyses, courts in Pennsylvania should address text messages as their own entity.[136] To make this shift, courts should begin to follow the reasoning of the Washington State Supreme Court in *Hinton*.[137] Despite text messages being "more vulnerable to invasion," the privacy interests in them should not vanish.[138] Instead, with advances in technology and greater surveillance, courts should begin to develop an approach

---

P.3d 9, 14 (explaining privacy rights overshadow needs of law enforcement in Washington), *cert. denied*, 135 S. Ct. 947 (2015) (mem.).

133. *See Diego*, 119 A.3d at 377 (comparing text messages to e-mails).

134. *See Warshak*, 631 F.3d at 284 (discussing importance of privacy in e-mails). The *Warshak* court used the second prong of the *Katz* test to determine whether society would find a reasonable expectation of privacy in e-mails, noting the importance of the question given the wide usage of email. *Id.* ("This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. . . . People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button.").

135. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2484–85 (2014) (noting technological advances do not make information less private); City of Ontario, v. Quon, 560 U.S. 746, 760–61 (2010) (discussing that wide-spread use of cell phones may strengthen case for privacy); *Hinton*, 319 P.3d at 15 (stating courts must acknowledge "realities of modern life" in addressing privacy issues); *see also* Vitale, *supra* note 18, at 1138 & n.210–11 (pointing to divorce litigation to show that people have expectation of privacy in text messages). Vitale writes that divorce litigation includes many instances where "intimate text messages" are at issue. *See id.* at 1138 (discussing privacy expectation through divorce litigation). Practitioners have also cited a rise in text messages being used as evidence. *See id.* Vitale argues that there is "an expectation [in] society that text messages are a safe mode of communication for highly private affairs, even though such messages are often used as evidence in litigation." *Id.*

136. *See* Stillwagon, *supra* note 60, at 1202 (arguing courts should not force "analogies between objects just to make their analysis simpler"). Stillwagon argues that the facts of each case should factor into a court's decision. *See id.* (advocating for courts to take facts into consideration). Because cell phones contain "vast amounts of information" courts have to address warrantless cell phone searches as different from other searches, such as searching a container. *See id.* at 1200–01 (discussing wealth of information stored on cell phones).

137. *See Hinton*, 319 P.3d at 16 (finding reasonable expectation of privacy in text messages stored on another's phone).

138. *See id.* at 13 ("Text messages can encompass the same intimate subjects as phone calls, sealed letters, and other traditional forms of communication that have historically been strongly protected under Washington law.").

that protects privacy interests.[139]

This broad approach should follow interpretations of the Supreme Court's *Quon* and *Riley* decisions.[140] While the Court in *Quon* did not decide whether individuals have a reasonable expectation of privacy in a message they knowingly send to someone else, lower courts have interpreted the dicta in *Quon* to find an increasingly broad right to privacy in text messages.[141] It is a natural progression that the expectation of privacy should be expanded to encompass text messages sent and stored on another's phone.[142] In *Riley*, the Supreme Court acknowledged the need to expand privacy to cover text messages when it said cell phones contain many of the "privacies of life."[143] Even though people are able to carry this information in their hands, it does not make it "any less worthy of the protection for which the Founders fought."[144]

---

139. *See id.* (discussing advances in surveillance technology). The *Hinton* court noted that the state constitutional privacy protections are not analytically constrained or lessened because people anticipate lesser levels of protection. *See id.*

140. *See* Vitale, *supra* note 18, at 1110 n.3 (noting lower courts interpreted *Quon* holding to further encompass text messages). Vitale cites to a Missouri case, which held that individuals have an expectation of privacy in text messages, to prove courts have relied on *Quon* to find a reasonable expectation of privacy in text messages. *See id.* (citing State v. Clampitt, 364 S.W.3d 605, 609–10 (Mo. Ct. App. 2012)).

141. *See* City of Ontario, v. Quon, 560 U.S. 746, 765 (2010) ("Petitioners and respondents disagree whether a sender of a text message can have a reasonable expectation of privacy in a message he knowingly sends to someone's employer-provided pager. It is not necessary to resolve this question in order to dispose of the case, however."). While the Court did not address sent text messages (in discussing Quon's expectation of privacy in his own text messages the Court essentially assumed such an expectation existed), lower courts have relied on *Quon* to find a broad expectation of privacy in text messages. *See, e.g.*, United States v. Gomez, 807 F. Supp. 2d 1134, 1140 (S.D. Fla. 2011) (discussing *Quon* and noting "[a]s the weight of authority agrees that accessing a cell phone's call log or text message folder is considered a 'search' for Fourth Amendment purposes, it would *logically follow* that an individual also has a reasonable expectation of privacy with respect to operational functions, such as making calls or exchanging text messages." (emphasis added)); United States v. Davis, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011) (discussing *Quon* and finding reasonable expectation of privacy in person's cell phone, including text messages); United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009) ("Cellular phones contain 'a wealth of private information' such as recent-call lists, emails, text messages, and photographs. An owner of a cell phone generally has a reasonable expectation of privacy in the electronic data stored on the phone. Thus, a search warrant is required to search the contents of a cell phone unless an exception to the warrant requirement exists." (citations omitted) (quoting United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008)).

142. *See Hinton*, 319 P.3d at 13–14 (discussing evolution of privacy issues from telegraphs, to phone calls, to electronic communications).

143. *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)) (internal quotation marks omitted) (discussing importance of privacy interests).

144. *See id.* at 2495 (discussing in dicta importance of privacy in United States). While discussing the Fourth Amendment and privacy, the Court refers to a 1761 James Otis speech opposing the British officers' "writs of assistance." *See id.* at 2494 (discussing reliance on Fourth Amendment by those in opposition to home searches during Colonial Era). John Adams, present at the speech, proclaimed "Otis's speech was 'the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'" *See id.* (quoting *Boyd*, 116 U.S. at 625); *see also Transcript: Read the Full Text of the Primetime Republican* Debate, *supra* note 2 (discussing importance of

This language demonstrates that much of the foundation of the United States is based in the rights of privacy, and Pennsylvania courts should be willing to use this language to find a broader expectation of privacy in sent text messages.[145]

While there are limited guidelines to follow, courts must attempt to adapt.[146] If courts continue to ignore and erode our expectations of privacy, "the essence of human freedom [will be] severely crippled."[147]

B. *Fixed Bug Causing App to Crash: Legislation Would Allow Law Enforcement to Fight Crime While Recognizing Important Privacy Interests*

To provide texters with an expectation of privacy, the Pennsylvania legislature will need to address the loophole in the Pennsylvania Wiretap Act that allows police officers to access messages via an informant without first obtaining a warrant.[148] The *Diego* court noted there would have been "a different legal question" had the police officers "observed the text message conversation over Appellee's shoulder as it occurred . . . ."[149] This had not

---

privacy, candidate Rand Paul said, "The Fourth Amendment was what we fought the Revolution over! John Adams said it was the spark that led to our war for independence . . . .").

145. *See* Stillwagon, *supra* note 60, at 1206 (arguing cell phones are unique and courts should "recognize the nuances of modern cell phone technology"); *see also* Vitale, *supra* note 18, at 1144 ("Despite the continuing evolution of electronic communication, the Court cannot ignore that text messaging has come to play a vital role in American society as a prevalent way to convey private information.").

146. *See* Vitale, *supra* note 18, at 1143–44 (noting future will bring new challenges with new forms of communication).

147. *See* Greenwald, *supra* note 1 (criticizing notion that privacy is not important). In his speech, Greenwald opposes "the idea that only people who are doing something wrong have things to hide and therefore reasons to care about privacy . . . ." *See id.* Nevertheless, he argues that those in power have "a much narrower conception of . . . 'doing bad things.' For them, 'doing bad things' typically means doing something that poses meaningful challenges to the exercise of our own power." *See id.* Further, he says that failing to challenge constraints does not make them "any less potent." *See id.* (claiming that ignoring mass surveillance "chains" does not make them weaker). Finally, he concludes by quoting activist Rosa Luxemburg by saying, "He who does not move does not notice his chains." *See id.* (internal quotation marks omitted).

148. *See* Nelson, *supra* note 22 (arguing fine line exists between interception and no interception in *Diego*).

149. *See* Commonwealth v. Diego, 119 A.3d 370, 381–82 (Pa. Super. Ct. 2015) (discussing whether outcome would be different with different facts), *appeal denied*, 129 A.3d 1240 (Pa. 2015) (mem.) (unpublished table decision). The *Diego* court found the assertion from Diego—that the police officers were observing the text messages as they were sent to Still's phone—was not supported by the facts. *See id.* (asserting record does not support Appellee's assertion). In a footnote, the court provided the testimony of the detective as well as the suppression court opinion and Diego's brief and said that the suppression court never definitively found that the officers observed the messages. *See id.* at 381 n.2. "Detective Moyer testified that Officer Corey Dickerson was sitting next to Mr. Still during the communications and said that it was possible that the officer observed what Mr. Still was doing on the iPad." *Id.* (quoting Transcript of Proceedings, Suppression Hearing - Vol. 3, at 1–2, Commonwealth v. Diego (C.P. Dauphin Mar. 16, 2015), No. 22–CR–0001203–2013 [hereinafter Transcript of Suppression Hearing]). The superior court, in dismissing this

occurred, so no interception occurred in violation of the Pennsylvania Wiretap Act.[150]

The fact that the actions taken by police did not constitute an interception reveals a major flaw in the Pennsylvania Wiretap Act.[151] The court was correct in dismissing the Commonwealth's reliance on *Proetto* and *Cruttenden* and arguing the amount of "police intrusion" determined whether an interception occurred.[152] However, by relying on the Commonwealth's assertion that Still "voluntarily" turned over the text messages ignores that law enforcement often coerce informants into turning over messages under the threat of arrest.[153] When the police apprehended Still, Still was asked to set up a drug deal with Diego, and the police told Still "it would be in his best interest to do so."[154] Still had no choice but to comply with the officers' demands.[155]

Other courts addressing similar issues have held it should almost always be a requirement for law enforcement to obtain a warrant to search someone's information.[156] While the *Diego* court found that the police did not intercept

possibility, stated, "The mere possibility that Officer Dickerson had contemporaneously observed the conversation between Appellee and Still on Still's iPad does not demonstrate that he did observe it. It merely expresses Detective[] Moyer's uncertainty about what Officer Dickerson observed." *Id.*

150. *See id.* at 380 (holding no interception occurred). Because Still, and not the police, spoke with Diego, the communication ended as soon as Still received the text message, and therefore the police could not have intercepted it. *See id.* at 380–81.

151. *See id.* (discussing that no interception occurred because Still relayed text messages to police).

152. *See id.* (rejecting Commonwealth's argument). "The definition of 'intercept' in Section 5702 specifically excludes 'the acquisition of the contents of a communication . . . between a person and an investigative or law enforcement officer, where the investigative or law enforcement officer poses as an actual person who is the intended recipient of the communication[.]'" *Id.* (second alteration in original) (quoting 18 PA. CONS. STAT. ANN. § 5702). Based off this language, the court found that the exception to the definition of *intercept* in the statute did not apply; nonetheless, the court held no interception occurred at all. *See id.*

153. *See id.* (noting Still "voluntarily" relayed text messages to police). The court found that Still spoke directly with the appellee by text message. *See id.* Further, the court found that this conversation was voluntary. *See id.* Because Still was the one speaking with Diego, "he could not be said to have intercepted it simply because he received it. That he subsequently relayed the contents of that conversation to the police does not render either his or the police's conduct an 'interception' under the plain meaning of the Act." *See id.* at 380–81; *see also* Richard Q. Hark, *Your IPAD and Text Communications . . . No Expectation of Privacy . . . Sanctioned Police Conduct*, HARK & HARK (July 23, 2015), https://penncriminaldefense.wordpress.com/2015/07/23/your-ipad-and-text-communications-no-expectation-of-privacy-sanctioned-police-conduct/ [https://perma.cc/9QCY-NLEG] (criticizing result in *Diego* and noting police likely observed text messages).

154. *See Diego*, 119 A.3d at 372 (citing Transcript of Suppression Hearing, *supra* note 150, at 1–2) (explaining officers' request that Still set up heroin deal with Diego).

155. *See Your IPAD and Text Communications*, *supra* note 153 (criticizing holding in *Diego*). The author argues that "police participate in [criminal informant] real-time texting all the time. . . . The [*Diego*] court ignored reality." *See id.* (arguing that police should have been required to secured warrant).

156. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."); *see also* United States v. Warshak, 631 F.3d 266, 288

Diego's text messages, the police officers' actions should be classified as an interception and reviewed under the Pennsylvania Wiretap Act.[157] Although it is important for law enforcement to maintain the ability to fight crime, privacy issues cannot be ignored; therefore, the Pennsylvania legislature should enact an amendment requiring law enforcement to obtain a warrant before enlisting an informant to relay text messages.[158]

V. CONCLUSION

As more and more courts find an increasingly broad expectation of privacy in text messages, it is natural to assume a greater expectation of privacy in sent text messages stored on another's phone.[159] The Supreme Court has noted that it is important to recognize the privacy rights in new forms of technology.[160] As text messages contain the "privacies of life," they should be afforded a reasonable expectation of privacy from unwarranted government intrusion.[161] The Pennsylvania Wiretap Act needs to be amended to limit the ability of law

(6th Cir. 2010) ("The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."); State v. Hinton, 319 P.3d 9, 16 (Wash. 2014) (en banc) ("Law enforcement is certainly permitted to use some deception, but '[e]xperience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.'") (alterations in original) (quoting Chandler v. Miller, 520 U.S. 305, 322 (1997), *cert. denied*, 135 S. Ct. 947 (2015) (mem.).

157. *See* Nelson, *supra* note 22 (arguing *Diego* allows for easier warrantless searches). Nelson writes, "For now, perhaps, the answer is, 'don't text with an informant,' but this shifts the focus to citizens to remain vigilant from government overreaching, rather than on the government to uphold its obligations." *Id.*

158. *See* Stillwagon, *supra* note 60, at 1205–06 (discussing purpose of Fourth Amendment). However, the Fourth Amendment allows law enforcement officers to use evidence. *See id.* (explaining use of evidence under Fourth Amendment). It just ensures that a "neutral and detached magistrate" will make inferences about possible evidence, allowing the law enforcement officer to legally fight crime. *See id.* at 1205–06 (quoting Johnson v. United States, 333 U.S. 10, 13–14 (1948)).

159. *See* Vitale, *supra* note 18, at 1144 (arguing new forms of electronic communication will continue to develop). Vitale argues for a "uniform body of law surrounding text messages" that will enable courts in the future to address text message privacy without having to rely on tenuous analogies. *See id.* (emphasizing need for uniformity in law concerning text messages and privacy).

160. *See Warshak*, 631 F.3d at 285 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)) (discussing necessity of Fourth Amendment keeping pace with technology).

161. *See Riley*, 134 S. Ct. at 2494–95 ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" (citation omitted) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). The Court writes that because the Fourth Amendment is one of the founding principles of the United States, it should only be circumvented by the use of warrantless searches in limited "exigent circumstances." *See id.* at 2494. Examples of this would include "a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone." *See id.* Nevertheless, because the Fourth Amendment is one of the founding principles of the United States, it should only be circumvented in these rare situations. *See id.*

enforcement to infringe on this right to privacy.[162] Until the Pennsylvania courts acknowledge a right to privacy in sent text messages and until the legislature amends the Pennsylvania Wiretap Act, residents of the Commonwealth may need to abide by words of caution—Don't Press Send.[163]

162. *See* Commonwealth v. Diego, 119 A.3d 370, 381–82 (Pa. Super. Ct. 2015) (stating outcome of case may have been different with slightly different facts), *appeal denied*, 129 A.3d 1240 (Pa. 2015) (mem.) (unpublished table decision); *see also* Nelson, *supra* note 22 (arguing unclear law may lead to government overreach).

163. *See* Nelson, *supra* note 22 (warning not to text with informant).