


March 2016

## Show Me The Warrant: Protection Of Stored Electronic Communications In New York State

Kaitlin G. Klamann

*Fordham University School of Law*

Follow this and additional works at: <https://ir.lawnet.fordham.edu/ulj>

 Part of the [Fourth Amendment Commons](#), [National Security Law Commons](#), [Privacy Law Commons](#), and the [State and Local Government Law Commons](#)

---

### Recommended Citation

Kaitlin G. Klamann, *Show Me The Warrant: Protection Of Stored Electronic Communications In New York State*, 41 Fordham Urb. L.J. 1407 (2014).

Available at: <https://ir.lawnet.fordham.edu/ulj/vol41/iss4/3>

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Urban Law Journal by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact [tmelnick@law.fordham.edu](mailto:tmelnick@law.fordham.edu).

**SHOW ME THE WARRANT:  
PROTECTION OF STORED ELECTRONIC  
COMMUNICATIONS IN NEW YORK STATE**

*Kaitlin G. Klamann\**

Introduction .....	1408
I. Background .....	1414
A. What Is Eavesdropping? .....	1414
B. What Are “Stored Electronic Communications”? .....	1416
C. The Federal Framework.....	1417
1. The Wiretap Act.....	1418
2. The Stored Communications Act.....	1420
D. New York’s Framework.....	1422
1. Obtaining an Eavesdropping Warrant in New York	1423
2. Obtaining a Search Warrant Under New York Law.	1425
II. The Conflict .....	1425
A. The Statute’s Plain Language .....	1426
B. The Courts’ Interpretation.....	1427
III. New York Law Should Require an Eavesdropping Warrant for Law Enforcement’s Access to All Stored Electronic Communications .....	1430
A. Law Enforcement Access to Stored Communications in New York Should Not Require an Eavesdropping Warrant .....	1430
1. The Threat Posed to Individual Privacy Rights Is Not as Great for Stored Electronic Communications as it Is for in-Transit Electronic Communications.....	1431
2. Requiring an Eavesdropping Warrant for Access to Stored Electronic Communications Would Overburden Law Enforcement Officials .....	1432

---

\* J.D. Candidate 2014, Fordham University School of Law. B.A. 2010 University of Chicago. For guidance, I am very grateful to Professor Deborah Denno of Fordham Law School and the amazing staff of the *Fordham Urban Law Journal*.

B.	New York Should Enact a Warrant Requirement for Stored Electronic Communications .....	1435
1.	Reasonable Expectation of Privacy in Electronic Communications.....	1435
a.	The Third-Party Doctrine Should Not Defeat Fourth Amendment Protection of Stored Electronic Communications .....	1436
b.	Society Has an Objectively Reasonable Expectation of Privacy in Stored Electronic Communications .....	1439
2.	Requiring a Search Warrant Will Not Over-Burden Law Enforcement Officials .....	1441
3.	Requiring a Search Warrant for Access to Stored Electronic Communications Would Eliminate Confusion Over the Distinctions Contained in the SCA and Pressure Congress to Take Action .....	1442
IV.	The Proposed Revision .....	1443
A.	Changes to the Language of New York Penal Law Section 250.00 and New York Criminal Procedure Law Section 700.05.....	1444
B.	Proposed Statute Requiring a Search Warrant for Law Enforcement Access to Stored Electronic Communications .....	1446
Conclusion.....		1449

## INTRODUCTION

In June 2013, Americans were stunned to discover that the government was spying on their Internet activities.<sup>1</sup> Edward Snowden, a former National Security Administration (NSA) contractor,<sup>2</sup> initially revealed to The Guardian, a national British daily newspaper, that the NSA was using a program called Prism to gain access to Americans' emails and online data through their Internet service providers (ISPs).<sup>3</sup> Specifically, the NSA was using

---

1. See Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES, June 9, 2013, <http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html>; Charlie Savage et al., *U.S. Confirms That It Gathers Online Data Overseas*, N.Y. TIMES, June 6, 2013, <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html>.

2. See Mazzetti & Schmidt, *supra* note 1.

3. See Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 7, 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. The Prism

this program to tap into the central servers of several leading U.S. Internet companies, extracting private audio and video chats, photographs, e-mails and other documents stored online.<sup>4</sup>

While the Foreign Intelligence Surveillance Act (FISA),<sup>5</sup> which allows the NSA to conduct surveillance on matters of *foreign* intelligence,<sup>6</sup> is the statute at the heart of the scandal, the debate that the scandal has generated about government surveillance also draws attention to problems in our *domestic* surveillance laws. Our domestic surveillance laws, which exist both on the federal and state level, provide for government surveillance of American citizens by law enforcement officials. The current legal framework, enacted on the federal level and copied in many states, is significantly outdated and therefore woefully inadequate to protect Americans' privacy in modern communications like email and text messaging.

Specifically, the current federal statute, the Electronic Communications Privacy Act (ECPA)<sup>7</sup> was enacted in 1986, when the Internet was still in its infancy.<sup>8</sup> As a result, protection of stored e-mail and text messages is so weak today that government officials are often able to access thousands of these private communications without a showing of probable cause.<sup>9</sup> This weakness is true on the federal level and in many states. This Note focuses on New York's surveillance framework, which tracks the ECPA, pointing out weaknesses in New York's framework with respect to government access to stored electronic communications like text-messages and emails.

---

program allows the NSA to collect the communications of users of these ISPs. Under the governing law, the NSA can gain access to accounts of users who live outside the United States. The NSA can also access the accounts of Americans whose communications include people outside the United States.

4. See Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, [http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html](http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html).

5. The Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–12 (Supp. 2011).

6. See *id.*

7. See Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22, 2701–12, 3121–27 (2012).

8. See generally William Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195 (2010).

9. See generally *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Specifically, the Stored Communications Act allows government access to certain stored electronic communications if the government simply procures a court order or subpoena. See 18 U.S.C. § 2703 (2012).

Given the growing prevalence of and reliance upon these modes of communication, government access to these messages upon such a low showing is troubling to say the least. In fact, today many Americans prefer to communicate via email or text message over other communication mediums. Specifically, one recent study found that young adults connect just as often through electronic communications as they do in-person.<sup>10</sup> Similarly, in 2011 thirty-one percent of text message users stated that they preferred texting to speaking on the phone.<sup>11</sup> The irony of these statistics is that Americans' in-person conversations or telephone conversations are much more protected from government intrusion than electronic communications.<sup>12</sup> Even though Americans are beginning to use electronic modes of communication more often and to convey the same information as they have traditionally conveyed in-person or via telephone, those electronic messages are more vulnerable to government surveillance.

At this point, many readers might respond, "So what? If the government has to read my emails or texts in order to prevent acts of violence or terrorism, that's ok with me. I have nothing to hide. I will gladly surrender my privacy if it means that Americans are safe." These readers are not wrong. It is about balance. It is about determining *when* the government can violate an individual's privacy rights in order to prevent and investigate crime. The current legal framework fails to strike the right balance. The following examples will demonstrate the dangers posed by the law's weaknesses.<sup>13</sup>

Joe Smith is an upstanding citizen and pillar of his community. He is married to a well-respected woman and is a father to three children. Unfortunately, Joe's brother, Dave, has gotten mixed up in organized crime. Dave had agreed to be a witness for the prosecution in an upcoming trial against a mob boss but has since disappeared. The prosecution is desperate to find him. Convinced that he ran away and that his brother is sure to have knowledge of his whereabouts, the government gets a court order to search Joe's emails and text messages. The messages do not reveal any information about Dave's location but they do reveal a series of explicit exchanges between Joe

---

10. *See generally* JON D. MILLER, UNIV. OF MICH., THE GENERATION X REPORT (2013).

11. PEW RESEARCH CTR., AMERICANS AND TEXT MESSAGING 1 (2011).

12. *See infra* Part I.C. and Part I.D.

13. These examples are hypothetical, created by the author for the purpose of demonstrating potential situations where the failings in the law could have real-life consequences for innocent individuals.

and several women. Still convinced that Joe knows the location of a vital witness, the prosecution approaches him with their new information, threatening to expose the affair if Joe does not cooperate with the prosecution.

Additionally, consider Amy Miller. Amy is a single woman in her late twenties living in a small town. Amy is schizophrenic. She has been on medication for years without an episode and prefers that her community not know of her condition. The head of the company where Amy works is suspected of embezzlement. Investigators, for one reason or another, believe that Amy may have had knowledge of her boss's actions or even know what he did with the money. So local law enforcement officials, many of whom Amy knows and considers friends, get a court order for her emails and texts. The messages reveal that Amy has schizophrenia, and soon the whole town knows about her mental illness.

One final example<sup>14</sup> is Michael Williams. Michael is a young married man with a promising future. Michael is also Muslim-American. State police and the FBI have been conducting surveillance of Muslim individuals in his community ever since September 11, 2001. Their primary source of information is informants stationed within the Muslim communities. Investigators obtain a court order or subpoena to access Michael's emails and texts. They discover a number of pornographic messages and images exchanged between Michael and his wife before their marriage. If exposed, these actions would destroy Michael's reputation in the Muslim community. Investigators then use this information to force Michael to inform on the Muslim community.

In each of these hypothetical examples, government officials did not have to demonstrate probable cause to obtain the users' private electronic correspondence. Joe's emails and texts were searched without a showing that law enforcement had probable cause to believe that Joe had any knowledge of his brother's whereabouts. Amy's messages were turned over despite the fact that law enforcement could not demonstrate probable cause that she had any knowledge of her boss's actions. And finally, Michael's messages

---

14. This example is loosely based on a recent news story. See Alastair Jamieson, *Report: NSA Spied on Porn Habits to Discredit Muslim Radicals*, NBC NEWS (Nov. 27, 2013), [http://usnews.nbcnews.com/\\_news/2013/11/27/21637011-report-nsa-spied-on-porn-habits-to-discredit-muslim-radicals?lite](http://usnews.nbcnews.com/_news/2013/11/27/21637011-report-nsa-spied-on-porn-habits-to-discredit-muslim-radicals?lite). For an in-depth look at the use of informants by local and federal law enforcement officials in their investigations of Muslim communities, see generally MATT APUZZO & ADAM GOLDMAN, *ENEMIES WITHIN: INSIDE THE NYPD'S SECRET SPYING UNIT AND BIN LADEN'S FINAL PLOT AGAINST AMERICA* (2013).

were searched without any showing at all that his private information was related to an existing criminal investigation other than his status as a Muslim. Moreover, while law enforcement's use of these messages to force cooperation may verge on prosecutorial misconduct, the intrusion itself—the reading of the private information—is where the harm begins. These hypothetical examples highlight the fact that many Americans today communicate very private information via email and text message. Thus, government access to these private communications, even without any misuse of the information, is wrong. The intrusion upon individual privacy rights represented by government access to these communications has grown as society's reliance upon electronic communication has increased.

So what can be done to protect electronic communications? There seem to be two options: (1) the states can wait for guidance from the federal government via Congress or the courts, and in the meantime continue to allow the search of citizens' stored electronic messages without a warrant; or (2) the state legislatures can take action. Given that Congress has failed to enact an amendment to the ECPA despite the fact that an amendment has been proposed in each of the last three Congressional sessions,<sup>15</sup> the first option could leave Americans' privacy rights unprotected for a long time. Similarly, the Supreme Court has failed to provide guidance<sup>16</sup> and the lower courts are churning out conflicting opinions that rely on outdated distinctions.<sup>17</sup>

---

15. A bill to amend the Electronic Communications Privacy Act was introduced in Congress in each of the last three years. This year's attempt is still pending in both the House and Senate. See *H.R. 2471 (112th)*, GOVTRACK.US, <https://www.govtrack.us/congress/bills/112/hr2471> (last visited Mar. 15, 2014) (showing that the 2011 bill died in the Senate after passing in the House). Another bill was introduced in the House in 2012 but died in committee. See also *H.R. 6339 (112th): Electronic Communications Privacy Act Modernization Act of 2012*, GOVTRACK.US, <https://www.govtrack.us/congress/bills/112/hr6339> (last visited Mar. 15, 2014). There is also a bill to amend the ECPA currently before the Senate, however it has been stalled since April 25, 2013. See *S. 607: Electronic Communications Privacy Act Amendments Act of 2013*, GOVTRACK.US, <https://www.govtrack.us/congress/bills/113/s607> (last visited Mar. 15, 2014).

16. See generally *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010) (deciding the case purely on a reasonableness inquiry instead of the Fourth Amendment question). The Supreme Court declined to review a decision about protections for stored email messages in 2013. See *Jennings v. Broome*, 133 S. Ct. 1806 (2013) (denying certiorari).

17. See *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (reversing on procedural grounds a prior decision that held emails were protected under the Fourth Amendment); *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007) (holding that monitoring of non-content information stored with electronic communication service provider did not violate the Fourth Amendment).

The second option, on the other hand, would offer Americans protections by their states,<sup>18</sup> and may also pressure Congress to take action on the federal level. States can take action by enacting more protective legislation, whether that be in the form of an amendment of an already existing surveillance statute or whether that involves passing a new piece of legislation providing for the protection of electronic communications. In fact, the Texas state legislature recently took action to protect its citizens and amended its surveillance statute to implement a warrant requirement for all stored electronic communications.<sup>19</sup>

This Note argues that New York should follow Texas's lead and update its eavesdropping statute. In fact, a recent discrepancy between the plain language of New York's surveillance statute<sup>20</sup> and the state courts' interpretation of the statute<sup>21</sup> presents the legislature with the perfect opportunity to reconsider the statute's treatment of stored electronic communications as discussed in Part II.

Specifically, this Note recommends that New York's eavesdropping law be revised to require that state law enforcement officials procure a search warrant before they search an individual's stored electronic communications such as emails and texts. This Note demonstrates that this solution is the best way to strike the correct balance between individual privacy rights and law enforcement efficacy.

Part I of this Note provides background information on the law of eavesdropping generally. It also discusses New York's eavesdropping law and the current federal legal framework. Part II examines the conflict in New York between the plain language of New York's eavesdropping statute and the courts' interpretation of New York's eavesdropping statute. Part III advocates for the elimination of stored electronic communications from the eavesdropping statute. It further proposes that law enforcement access to these communications should require a search warrant under New York law. Finally, Part IV suggests specific revisions to New York's law to effect this Note's suggestions.

---

18. State statutes will not protect their citizens from electronic surveillance from federal law enforcement officials.

19. See TEX. CODE CRIM. PROC. ANN. art. 18.02 (West 2013); Bob Sullivan, *Don't Mess With Texas Email: State Law Ends Some Warrantless Email Searches*, NBC NEWS (June 18, 2013), [http://redtape.nbcnews.com/\\_news/2013/06/18/19025074-dont-mess-with-texas-email-state-law-ends-some-warrantless-email-searches?lite](http://redtape.nbcnews.com/_news/2013/06/18/19025074-dont-mess-with-texas-email-state-law-ends-some-warrantless-email-searches?lite).

20. N.Y. PENAL LAW §250.00(6) (McKinney 2013) (defining "intercepting or accessing of an electronic communication").

21. See *Gurevich v. Gurevich*, 886 N.Y.S.2d 558 (Sup. Ct. 2009); *Moore v. Moore*, N.Y. L.J., Aug. 14, 2008, at 26; *Boudakian v. Boudakian*, N.Y. L.J., Dec. 26, 2008.



## I. BACKGROUND

This Part provides background information on eavesdropping laws generally. Part I.A explains what the term “eavesdropping” means, why it is generally prohibited and why we allow government officials to eavesdrop under limited circumstances. Part I.B explores the technical process of sending email and text messages in order to provide background information necessary to understanding the distinctions made in the federal framework. Part I.C discusses the federal framework, emphasizing the various distinctions that the law makes with respect to electronic communications. This discussion is important to understand the New York courts’ interpretation of the statute and the nature of the debate over the treatment of electronic communications. Finally, Part I.D lays out New York’s eavesdropping law. It describes the process of procuring an eavesdropping warrant in New York, including a discussion of the showings required by law enforcement in order to obtain the contents of communications.

### A. What Is Eavesdropping?

Blackstone defines eavesdroppers those who “listen under walls or windows, or the eaves of a house, to hearken after discourse.”<sup>22</sup> While eavesdropping methods are much more sophisticated today than in Blackstone’s time, the basic concept is the same: eavesdropping is the act of listening in on a person’s personal communications, often unbeknownst to the speaker. And while private individuals are certainly capable of eavesdropping, the government is often the biggest perpetrator of all, as recent events have demonstrated.<sup>23</sup>

Both state<sup>24</sup> and federal laws<sup>25</sup> generally prohibit eavesdropping. Nevertheless, the government is allowed to eavesdrop under specific circumstances if it meets certain legal thresholds under the applicable law. Specifically, the federal framework<sup>26</sup> contains three different levels of protection, each requiring the government to meet a distinct legal threshold. The highest standard is an eavesdropping warrant.

---

22. 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 169 (1769).

23. See Mazzetti & Schmidt, *supra* note 1; Savage et al., *supra* note 1.

24. For example, this Note deals with the New York eavesdropping framework contained in N.Y. PENAL LAW § 250.00 (McKinney 2013) and N.Y. CRIM. PROC. LAW §§ 700.05–.70 (McKinney 2013).

25. The controlling federal law is the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22, 2701–12, 3121–27 (2012).

26. See *id.*

Communications requiring an eavesdropping warrant are considered to have the greatest privacy interests at stake and are therefore awarded the most protection.<sup>27</sup> The next standard requires law enforcement to obtain a search warrant before they are given access to certain communications.<sup>28</sup> Finally, the lowest standard requires law enforcement officials to merely obtain an administrative subpoena or court order. If law enforcement officials meet the requisite legal standard, they are permitted to intercept or access these communications. These standards are mirrored in New York's surveillance law, as discussed in greater depth below.<sup>29</sup>

The varying standards represent the balance struck between law enforcement's interests and individuals' privacy interests.<sup>30</sup> Advances in communications technology often and easily disrupt this delicate balance. If eavesdropping laws fail to keep up with these advances, and the delicate balance is upset, there is potential for serious consequences, both for individual civil liberties and law enforcement. The growing prevalence of electronic communications like email and text messaging is one such advance in technology whose outdated treatment under the law of eavesdropping has upset this fragile balance.<sup>31</sup>

---

27. See Orin Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 621 (2003). These thresholds range from least protective (no legal process or subpoena) to a high level of protection (eavesdropping warrant). See *id.*

28. See Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012).

29. See *infra* Part I.C.

30. In fact, Congress recognized the need for this balance when they enacted the ECPA stating that the goal of the ECPA was twofold: to preserve “a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.” H.R. REP. NO. 99–647, at 19 (1986).

31. See generally Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121; Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004); Katharine M. O'Connor, *:0 OMG They Searched My Txts: Unraveling the Search and Seizure of Text Messages*, 2010 U. ILL. L. REV. 685; Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349 (2009); Ric Simmons, *Can Winston Save Us From Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches*, 55 RUTGERS L. REV. 547 (2003).

## B. What Are “Stored Electronic Communications”?

This Note is primarily concerned with two types of electronic communications—email messages and text messages—and their treatment under New York’s eavesdropping law.<sup>32</sup> To understand the distinctions the New York courts (and the ECPA) have made with respect to these communications, it is important to understand the mechanics of their transmission.

The nature of email has changed significantly over the last few decades. When Congress first passed the ECPA in 1986, web-based email systems like Gmail and Yahoo!Mail did not yet exist.<sup>33</sup> Instead, email primarily existed in local intranets where users would download their messages from a server to their own computer.<sup>34</sup> Copies of email messages already received and read would then remain on the individual’s computer rather than on a remote server.<sup>35</sup>

Today, many email services are web-based.<sup>36</sup> Emails are sent using a collection of computer servers operated by ISPs that work together and function as a single system.<sup>37</sup> Each ISP has the task of running applications and storing data in small pieces before it passes that data on to the next server in line.<sup>38</sup> After a user composes and sends an email, the message is broken up into small packets and distributed, stored, and transported among different servers until they are reconfigured with the recipient. Once the messages are received, they are stored in remote storage on the service provider’s server.<sup>39</sup> So instead of subscribing to a network like America Online and downloading emails from that network’s server onto a personal computer, today’s web-based email systems store received emails on a remote ISP server.<sup>40</sup>

Text messages go through a similar process. Cellular phones that are enabled for text messaging contain Short Message Service (SMS)

---

32. For a more in-depth discussion of email technology and its interplay with the SCA, see Courtney Bowman, *A Way Forward After Warshak: Fourth Amendment Protections for E-Mail*, 27 BERKELEY TECH. L.J. 809, 815–16 (2012).

33. See Robison, *supra* note 8, at 1197–98.

34. See *id.* at 1198.

35. See *id.*

36. See *id.* at 1199 (defining “cloud computing” as “the ability to run applications and store data on a service provider’s computers over the Internet, rather than on a person’s desktop computer”); see also Bowman, *supra* note 32, at 815–16.

37. See Robison, *supra* note 8, at 1200.

38. See *id.* See also Bowman, *supra* note 32, at 815–16.

39. See Robison, *supra* note 8, at 1200; Bowman, *supra* note 32, at 815–16.

40. This evolution to web-based e-mail, in which e-mails are stored with an ISP, is significant to the discussion of the third party doctrine *infra* Part III.

technology.<sup>41</sup> After a sender enters a message into his phone and sends it, the message is transmitted to a Short Message Center (SMC), where it is temporarily stored.<sup>42</sup> The SMC then sends the message to the recipient's mobile device.<sup>43</sup> If the receiving phone is unavailable, the SMC queues the message and attempts to send it again.<sup>44</sup> A sent message can be stored in both the sender's phone and the recipient's phone.<sup>45</sup> The message will remain on these devices until a user manually deletes it or it deletes automatically to make room for new messages.<sup>46</sup> The service provider also stores copies of the messages on its server.<sup>47</sup>

Thus, email and text messages go through varying stages of transition, reception and storage. Under the current federal framework, as discussed in Part I.C., the standard that law enforcement officials have to meet differs depending on what stage the messages are in.

### C. The Federal Framework

New York courts have interpreted the State's eavesdropping statute to reflect the federal framework's distinction between electronic communications that are in-transit and electronic communications that are in storage. This Subpart will explore the federal framework, as an understanding of this distinction is necessary to understand the New York courts' position.

On the federal level, the ECPA<sup>48</sup> governs federal law enforcement's access to a person's personal electronic communications.<sup>49</sup> Congress enacted the ECPA in 1986 to expand and revise Title III of the Omnibus Crime Control and Safe Streets Act (Title III).<sup>50</sup> Specifically, the ECPA extended some of the

---

41. See O'Connor, *supra* note 31, at 688. This Note does not discuss law enforcement access to texts via cell phones. Instead, this Note is concerned with the procurement of copies of texts from service providers.

42. See *id.*

43. See *id.*

44. See *id.*

45. See *id.*

46. See *id.*

47. See *id.*

48. See Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22, 2701–12, 3121–27 (2012).

49. The ECPA should not be confused with the Foreign Intelligence Surveillance Act (FISA), which establishes a separate legal regime for “foreign intelligence” surveillance. See 50 U.S.C. §§ 1801–85 (Supp. 2011). The ECPA outlines guidelines regulating ordinary law enforcement surveillance within the United States.

50. See Scolnik, *supra* note 31, at 375.

protections of Title III to electronic communications.<sup>51</sup> The ECPA created several distinctions for electronic communications based on the kind of information sought and the stage of transmission, as discussed below.

The ECPA is composed of three parts: (1) the Wiretap Act;<sup>52</sup> (2) the Stored Communications Act (SCA);<sup>53</sup> and (3) the Pen Register Act.<sup>54</sup> Generally, the Wiretap Act governs the interception of “wire,” “oral,” and “electronic” communications that are in-transit.<sup>55</sup> The SCA governs access to communications that have been received and stored, like stored voicemail messages, emails and text messages.<sup>56</sup> Finally, the Pen Register Act regulates the use of pen registers trap and trace devices. Trap and trace devices and pen registers identify the phone number of an incoming call or the outgoing phone numbers of calls placed from a particular phone, respectively.<sup>57</sup>

### 1. *The Wiretap Act*

The Wiretap Act governs law enforcement access to communications while those communications are still in transmission. Specifically, the Wiretap Act prohibits any person from intentionally intercepting any wire, oral or electronic communication.<sup>58</sup> Therefore, an interception is only a violation of the Wiretap Act if the communication fits into one of three categories. A “wire communication” is a conversation that takes place via telephone.<sup>59</sup> An “oral communication” is a face-to-face conversation in which the speakers have a reasonable expectation of privacy.<sup>60</sup> “Electronic communications” encompass communication via computer, including data transmission.<sup>61</sup> In effect, any conversation, either over the phone

---

51. See Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 41–42 (2004).

52. 18 U.S.C. §§ 2510–22 (2012).

53. *Id.* §§ 2701–12.

54. *Id.* §§ 3121–27. This Note is primarily concerned with the Wiretap Act and the Stored Communications Act, as these two statutes govern law enforcement access to electronic communications like e-mails and text-messages.

55. §§ 2510–22.

56. §§ 2701–12.

57. See GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 98-327, PRIVACY: AN ABBREVIATED OUTLINE OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 46 (2012). This Note focuses on electronic communications and therefore, the Pen Register Act will not be analyzed.

58. § 2511(1).

59. See STEVENS & DOYLE, *supra* note 57, at 12.

60. *See id.*

61. *See id.*

or in person, or any electronic communication that has not yet been received by the recipient, falls within the Wiretap Act. The prohibited interception is limited to the *contents* of these communications as opposed to non-content information like the caller or receiver's phone numbers.<sup>62</sup>

Government officials are exempt from the prohibitions against interception contained in the Wiretap Act when they procure an eavesdropping warrant,<sup>63</sup> or when they get the consent of one of the parties to the communication.<sup>64</sup> Obtaining an eavesdropping warrant requires law enforcement officials to meet the highest legal standard under the ECPA.<sup>65</sup> Thus, the Wiretap Act protects these in-transit communications above all others. The Wiretap Act also requires that state wiretapping laws be at least as protective as the federal law or risk invalidation under the Supremacy Clause of the Constitution.<sup>66</sup> Therefore, New York, in considering a revision to its eavesdropping laws, must continue to require state law enforcement officials to obtain an eavesdropping warrant for the interception of wire, oral or electronic communications that are in-transit,<sup>67</sup> as discussed in Part IV.

---

62. The Wiretap Act defines "contents" as "any information concerning the substance, purport or meaning of that communication." 18 U.S.C. § 2510(8) (2012). The SCA allows the government to obtain non-content basic subscriber information with a subpoena. Basic subscriber information includes the subscriber's name, address, and telephone number. See Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1219–20 (2004).

63. See 18 U.S.C. §§ 2516–18 (2012); STEVENS & DOYLE, *supra* note 57, at 23. To obtain an eavesdropping warrant, the attorney general, or someone authorized to act in his absence must file an application to an authorized judge. The application must include the identity of the officer, a full and complete statement of facts, a statement detailing other investigative procedures that have been tried and failed, a statement detailing the period of time required for the interception and a statement detailing previous applications for interception involving the same persons. See § 2518(1).

64. See 18 U.S.C. § 2511(2)(c) (2012).

65. See § 2518(3); see also *infra* Part I.D.1.

66. See U.S. CONST. art. 6, cl. 2; 18 U.S.C. § 2516(2). In other words, state statutes must require an eavesdropping warrant for those electronic communications that are in-transit because the Wiretap Act requires it.

67. See *supra* Part III.B.3. However, the Wiretap Act does not require an eavesdropping warrant for stored electronic communications. See Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012). Therefore, if New York's eavesdropping statute was revised to exclude stored electronic communications, that revision would satisfy the minimum federal constitutional criteria established by the Wiretap Act. See § 2516(2). However, any revision to exclude electronic communications altogether from the reach of the eavesdropping statute, thus eliminating the in-transit-versus-stored distinction, would violate the Supremacy Clause of the U.S. Constitution.

If a communication is not in-transit but instead has already been received and/or stored by the recipient, its treatment will be determined under the Stored Communications Act (SCA).

## 2. *The Stored Communications Act*

The SCA governs law enforcement access to electronic communications that are stored with a service provider.<sup>68</sup> The SCA prohibits law enforcement from intentionally accessing a service provider's facility without authorization in order to access a wire or electronic communication while it is in electronic storage.<sup>69</sup> Under the SCA, "service providers" would include SMCs and ISPs, as discussed above.<sup>70</sup> The SCA prohibits accessing the contents of stored text messages and emails in the records of these providers.

Just like the Wiretap Act, the SCA provides an exemption for law enforcement.<sup>71</sup> Law enforcement officials may compel service providers to produce copies of electronic communications that are stored on their server if they meet certain requirements under the SCA. As shown in the following paragraphs, the SCA is generally much less protective of these communications than the Wiretap Act.

The SCA creates several distinctions that determine what showing law enforcement officials must make to obtain access to stored communications.<sup>72</sup> First, the SCA distinguishes between two types of providers: what the SCA calls "Electronic Communication Service" (ECS) providers and "Remote Computing Service" (RCS) providers.<sup>73</sup> An ECS can hold content in "electronic storage" which is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission."<sup>74</sup>

---

68. See STEVENS & DOYLE, *supra* note 57, at 35. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (2012). Courts have concluded that law enforcement access to stored text messages is governed by the SCA. See *United States v. Jones*, 451 F. Supp. 2d 71, 76 (D.D.C. 2006), *rev'd on other grounds sub nom.*, *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

69. See § 2701(a).

70. See *supra* Part I.B.

71. See 18 U.S.C. § 2703 (2012).

72. This Note focuses on the distinctions made with respect to ECS and RCS providers, and those messages that have been stored for more than 180 days and those that have been stored for less than 180 days. For a more thorough exploration of the SCA, see Kerr, *supra* note 62.

73. See § 2703.

74. 18 U.S.C. § 2510(17)(A) (2012).

For example, a message that sits in an email inbox after transmission but before the user retrieves or reads the message is an example of ECS “electronic storage.”<sup>75</sup> Additionally, any time that a message is stored intermediately on its way to the recipient, that provider is considered an ECS provider under the SCA.<sup>76</sup>

Regarding RCS providers, the SCA defines RCS as “the provision to the public of computer storage or processing services by means of an electronic communication system.”<sup>77</sup> Files held in long-term storage after reception are protected under the rules for RCS providers.<sup>78</sup> Sometimes a provider can be considered a provider of both an RCS and an ECS, depending on the status of the particular communication that is the subject of the search.<sup>79</sup> In this way, the inquiry focuses on the provider’s role with respect to a particular communication.<sup>80</sup> One specific provider, therefore, may be a provider of ECS with respect to a certain communication or a provider of RCS with respect to another communication.<sup>81</sup>

If a provider is an ECS provider then the SCA creates a second distinction between those messages stored with an ECS provider for more than 180 days and those stored with an ECS provider for less than 180 days.<sup>82</sup> If the communication is held in storage with an ECS provider for less than 180 days, the government needs a search warrant in order to compel the provider to disclose it.<sup>83</sup> If the communication is in ECS storage for more than 180 days, the government may compel the provider to disclose it with a subpoena or court order.<sup>84</sup> If a communication is stored with an RCS, the government will also only need a subpoena or court order to compel the provider to disclose it, regardless of how long it has been in storage.<sup>85</sup>

---

75. See Fred Kemper, *Compulsion of Text Messages After Quon: Applying Old Law to New Technology*, 92 B.U. L. REV. 1381, 1386 (2012).

76. See Kerr, *supra* note 62, at 1216.

77. 18 U.S.C. § 2711(2) (2012).

78. See Kerr, *supra* note 62, at 1216.

79. See *id.* at 1215–16.

80. See *id.* at 1215.

81. See *id.* at 1215–16.

82. 18 U.S.C. § 2703(a) (2012).

83. *Id.*

84. § 2703(a)–(b), (d).

85. § 2703(b). Government officials can use a court order or subpoena only if they also give the user prior notice. See *id.* To obtain a § 2703 court order, the government must provide “specific and articulable facts showing that there are reasonable grounds to believe” that the information to be compelled is “relevant and material to an ongoing criminal investigation.” § 2703(d).



To see how these distinctions play out in practice, it may be helpful to return to the Joe Smith example. Under the SCA, law enforcement officials could access any of Joe's unopened emails or text messages that are on his ISP or SMC's servers for less than 180 days only with a search warrant.<sup>86</sup> However, if Joe's messages are unopened and stored on a server for more than 180 days, or opened at all (regardless of time stored) law enforcement agents can compel disclosure from Joe's service providers with a court order or a subpoena.<sup>87</sup>

Therefore, the Wiretap Act and the SCA create different regimes depending on whether the electronic communication sought is in-transit or is in storage. The Wiretap Act offers greater protection for electronic communications that are in-transit, while the SCA's distinctions based on the type of provider being used and the status of the message (opened, un-opened etc.) allow law enforcement officials to access stored electronic communications more easily.

#### D. New York's Framework

This Subpart lays out New York's current eavesdropping framework. Specifically, it discusses the procedures required under New York law in order to obtain both an eavesdropping warrant and a search warrant.

New York's eavesdropping statute, like many states' statutes, is heavily influenced by the ECPA. As a result, many of the requirements in New York mirror the requirements at the federal level. Unlike the ECPA, however, New York's framework does not consist of three separate statutes that mirror the Wiretap Act, the SCA and the Pen Register Act respectively. Instead New York has two statutes that address eavesdropping. One statute, in New York's penal law, criminalizes the act of eavesdropping by private individuals.<sup>88</sup> The second statute, in New York's criminal procedure law, governs eavesdropping by state law enforcement officers.<sup>89</sup> The latter statute, section 700 of New York's Criminal Procedure Law (section 700) will be the primary focus of this Note.

---

86. See Kerr, *supra* note 62, at 1223 tbl.

87. Email that is in electronic storage for more than 180 days can be accessed by either: (1) a subpoena with notice to the user, (2) a court order with notice to the user, or (3) a search warrant. See § 2703; see also Kerr, *supra* note 62, table on 1223.

88. See N.Y. PENAL LAW §§ 250.00–.65 (McKinney 2013).

89. See N.Y. CRIM. PROC. LAW §§ 700.05–.70 (McKinney 2013).

Like the federal Wiretap Act, the statute requires officials to obtain an eavesdropping warrant<sup>90</sup> or procure the consent of one of the parties to the communication<sup>91</sup> to access communications covered by the statute. However, New York does not contain a state statute that is the equivalent of the SCA. Therefore, treatment of stored electronic communications in New York is often determined according to the SCA.<sup>92</sup>

### 1. *Obtaining an Eavesdropping Warrant in New York*

New York's eavesdropping statute provides that law enforcement officials may intercept "a telephonic or telegraphic communication,"<sup>93</sup> "a conversation or discussion,"<sup>94</sup> or "electronic communications"<sup>95</sup> if the officials first obtain an eavesdropping warrant.

To obtain an eavesdropping warrant under New York's eavesdropping statute, the New York District Attorney, Attorney General, Deputy Attorney General, or anyone authorized to act on their behalf<sup>96</sup> must first file an ex parte application with the court.<sup>97</sup> The application must contain the following: (1) a statement of the applicant's identity and authority to make the application;<sup>98</sup> (2) a statement of the facts that justify the use of the warrant;<sup>99</sup> (3) a statement that the communications are not privileged; (4) a statement

---

90. *See id.* § 700.15.

91. *See id.* § 700.05(3).

92. *See e.g.*, *People v. Moorer*, 959 N.Y.S.2d 868, 875–76 (Sup. Ct. 2013); *People v. Harris*, 949 N.Y.S.2d 590, 594–96 (Crim. Ct. 2012).

93. *See* CRIM. PROC. § 700.05(3). This term is the equivalent of the term contained in the federal framework before being amended by the USA Patriot Act. The Patriot Act changed the term to "wire communication" to exclude voicemail messages from the Wiretap Act's framework.

94. *See id.*

95. *See id.*

96. *See* CRIM. PROC. § 700.05(5). This limitation is required under federal law. *See* 18 U.S.C. § 2516(2) (2012).

97. The term "justice" is defined by section 700 as any justice of an appellate division, supreme court, or county court of the judicial department or county in which the eavesdropping warrant is to be executed. *See* CRIM. PROC. § 700.05(4).

98. *Id.* § 700.20(2)(a).

99. CRIM. PROC. § 700.20(2)(b) ("including (i) a statement of facts establishing probable cause to believe that a particular designated offense has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted or the video surveillance is to be conducted, (iii) a particular description of the type of the communications sought to be intercepted or of the observations sought to be made, and (iv) the identity of the person, if known, committing such designated offense and whose communications are to be intercepted or who is to be the subject of the video surveillance.")

that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried; (5) a statement of the period of time for which surveillance is sought; and (6) a statement of any previous applications for surveillance of the same persons or places as are the subject of the current application.<sup>100</sup> These requirements are substantively identical to the showing required under federal law.<sup>101</sup>

After an application<sup>102</sup> is made to an authorized court,<sup>103</sup> the judge has discretion to decide whether to grant or deny the application.<sup>104</sup> The judge will evaluate the application to determine if: (1) there is probable cause to believe that a particular person is committing, has committed, or is about to commit a designated offense;<sup>105</sup> (2) there is probable cause to believe that particular communications concerning that offense will be obtained through eavesdropping;<sup>106</sup> (3) there is probable cause to believe that the place where the communications are to be intercepted is being used, or is about to be used, in connection with the commission of a designated offense.<sup>107</sup>

If the eavesdropping warrant issued is initially authorized to intercept communications as long as is necessary to achieve the objective of the authorization, it may not last longer than thirty days.<sup>108</sup> The thirty-day period begins no later than ten days after the warrant issues.<sup>109</sup> The warrant also contains a provision that requires

---

100. CRIM. PROC. § 700.20(2)(c)–(f).

101. The ECPA requires law enforcement to make the same showing. *See* United States v. Moran, 349 F. Supp. 2d 425, 453–55 (N.D.N.Y. 2005) (setting out the requirements for obtaining an eavesdropping warrant under federal law); *People v. Rabb*, 945 N.E.2d 447, 450 (N.Y. 2011) (“[I]t was the Legislature’s intention to conform state standards for court-authorized eavesdropping warrants with federal standards.” (internal quotation marks omitted)). *Compare* CRIM. PROC. § 700.20, with 18 U.S.C. § 2518 (2012).

102. In an emergency situation where imminent danger of death or serious injury exists, the statute does not require a written application but allows for an oral or electronic communication with an authorized justice. *See* N.Y. CRIM. PROC. LAW § 700.21(1) (McKinney 2013).

103. *See supra* note 97, discussing authorized courts.

104. *See* N.Y. CRIM. PROC. LAW § 700.25 (McKinney 2013). In determining whether or not an application should have been granted, appellate courts typically defer to the discretion of the issuing justice. *See e.g.*, *People v. Baker*, 577 N.E.2d 1064 (N.Y. 1991) (denying appeal of judgment based on sufficiency of eavesdropping warrant); *People v. Ianniello*, 554 N.E.2d 75 (N.Y. 1990).

105. *See* N.Y. CRIM. PROC. LAW § 700.15(2) (MCKINNEY 2013).

106. CRIM. PROC. § 700.15(3).

107. CRIM. PROC. § 700.15(5).

108. *See* CRIM. PROC. § 700.10(2). However, an applicant may file a request for an extension for an additional thirty days of surveillance. *See id.* § 700.40.

109. *See* CRIM. PROC. § 700.10(2).

surveillance be conducted in such a way as to minimize the interception of communications outside the scope of the surveillance.<sup>110</sup>

## 2. *Obtaining a Search Warrant Under New York Law*

Unlike the ECPA, New York's eavesdropping law does not contain a separate framework for stored communications. Instead, issuance of a search warrant is governed by section 690 of New York's criminal procedure law.<sup>111</sup>

The requirements for a search warrant differ from the higher requirements of an eavesdropping warrant in a few ways. A search warrant simply requires probable cause, meaning that the government must present facts establishing a likelihood that a crime has occurred and that evidence of the crime exists in the location to be searched.<sup>112</sup> Compared to an eavesdropping warrant, a search warrant does not require a showing that: (1) the heightened particularity requirement is satisfied; (2) "normal investigative procedures" have been tried and failed; (3) the surveillance will be conducted in a way that minimizes the interception of irrelevant information; (4) there is probable cause to believe the interception will reveal evidence of one of a limited number of specific crimes.<sup>113</sup>

## II. THE CONFLICT

This Part explores the current conflict in New York between the explicit language of the eavesdropping statute and the recent interpretation of the statute by the courts. Part II.A sets out the statutory language indicating that law enforcement in New York would need to obtain an eavesdropping warrant to compel disclosure of all electronic communications, regardless of whether or not they are in-transit or stored. Part II.B examines recent decisions by the New York courts interpreting the definition of "intercepting" to mean accessing electronic communications that are in-transit, not those communications that have been received and stored. Part II demonstrates that this conflict offers the New York legislature the chance to revise its statute to clarify the treatment of electronic communications under the state's eavesdropping law.

---

110. *See id.* § 700.30(9).

111. *See id.* §§ 690.05–.55.

112. *See* Kerr, *supra* note 27, at 620 tbl.; *see also* CRIM. PROC. § 690.35(3)(b); *People v. Vanness*, 965 N.Y.S.2d 227, 230 (App. Div. 2013).

113. *See* Simmons, *supra* note 31, at 553–54.

### A. The Statute's Plain Language

New York's eavesdropping statute<sup>114</sup> states that if law enforcement agents wish to intercept a person's private communications they must first obtain an eavesdropping warrant according to the procedure laid out in the statute.<sup>115</sup> Specifically the statute defines "eavesdropping" to include "'wired tapping', 'mechanical overhearing of conversation,' or the 'intercepting or accessing of an electronic communication', as those terms are defined in section 250.00 of the penal law."<sup>116</sup> Section 250.00 of the penal law defines each of those terms as follows:

"Wired tapping" means the intentional overhearing or recording of a telephonic or telegraphic communication by a person other than a sender or receiver thereof, without the consent of either the sender or receiver, by means of any instrument, device or equipment.<sup>117</sup>

"Mechanical overhearing of a conversation" means the intentional overhearing or recording of a conversation or discussion, without the consent of at least one party thereto, by a person not present thereat, by means of any instrument, device or equipment.<sup>118</sup>

"Intercepting or accessing of an electronic communication" and "intentionally intercepted or accessed" mean the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of the sender or intended receiver thereof, by means of any instrument, device or equipment . . . .<sup>119</sup>

Therefore, the statute prohibits three types of "eavesdropping": (1) wired tapping a telephone or telegraphic communication; (2) bugging or recording an in-person conversation; and (3) intercepting *or accessing* electronic communications. The language in (3) prohibiting eavesdropping by intercepting or accessing electronic

---

114. See N.Y. CRIM. PROC. LAW § 700.05(3) (McKinney 2013) (defining "intercepted communication" as including, "(a) a telephonic or telegraphic communication which was intentionally overheard or recorded by a person other than the sender or receiver thereof, without the consent of the sender or receiver, by means of any instrument, device or equipment, or (b) a conversation or discussion which was intentionally overheard or recorded, without the consent of at least one party thereto, by a person not present thereat, by means of any instrument, device or equipment; or (c) an electronic communication which was intentionally intercepted or accessed, as that term is defined in section 250.00 of the penal law").

115. See *supra* Part I.D.

116. CRIM. PROC. § 700.05(1).

117. N.Y. PENAL LAW § 250.00(1) (McKinney 2013).

118. PENAL § 250.00(2)

119. PENAL § 250.00(6).

communications is the key language that the courts have taken issue with, as discussed in Part II.B below.

The statute prohibits “intercepting *or accessing*” an electronic communication. The definition contains words like “acquiring, receiving, collecting” suggesting that it is not simply the contemporaneous interception of electronic communications while they travel from sender to recipient that is prohibited but also the *accessing* of such communications after they have been received. Therefore, the language of the New York eavesdropping framework fails to make the distinction between electronic communications that are stored and those that are in-transit.<sup>120</sup> Instead, the language indicates that law enforcement access to *any* type of electronic communication requires an eavesdropping warrant. However, courts interpreting the statute have determined that the statute *does* in fact only apply to those communications that are in-transit, despite the statute’s plain language.<sup>121</sup>

### B. The Courts’ Interpretation

Few cases have interpreted the language of New York’s eavesdropping law. In fact, the case law is silent as to whether or not law enforcement officials must procure an eavesdropping warrant to gain access to stored electronic communications.<sup>122</sup> However, New

---

120. Significantly, the ECPA simply uses the term “intercept” rather than New York’s “intercepting or accessing electronic communications.” This departure from the federal language suggests that the New York legislature, in drafting the statute in the shadow of the ECPA, made a conscious decision to depart from the federal framework.

121. *See* Gurevich v. Gurevich, 886 N.Y.S.2d 558 (Sup. Ct. 2009); Boudakian v. Boudakian, N.Y. L.J., Dec. 26, 2008 (Sup. Ct. 2008); Moore v. Moore, N.Y. L.J., Aug. 14, 2008 (Sup. Ct. 2008).

122. New York courts have heard similar inquiries. For example, in *People v. Harris*, the question was whether or not the government can compel Twitter to turn over the records of a user’s tweets. 949 N.Y.S.2d 590 (Crim. Ct. 2012). In that case, the defendant was charged with disorderly conduct after marching on the Brooklyn Bridge. *See id.* at 592. The prosecution sent a subpoena to Twitter seeking the defendant’s account information and relevant tweets. *See id.* The defendant moved to quash the subpoena but the court ruled against him, issuing a court order on Twitter for the information’s disclosure. Twitter then moved to quash the court order. *See id.* The court held that the Fourth Amendment did not protect the defendant’s tweets because the defendant intentionally broadcasted them to the public. *See id.* at 595. The court was careful to distinguish this case from a case concerning email or text messaging stating that this case “deals with tweets that were publicly posted rather than an e-mail or text that would be directed to a single person or a select few.” *Id.* at 590. Similarly, New York courts have also considered the question of whether government access to cell site location data without a search warrant is a violation of the Fourth Amendment. *See* *People v. Moorer*, 959 N.Y.S.2d

York's lower courts have recently been faced with interpreting the statute in the context of matrimonial actions.<sup>123</sup> In each of these cases, a spouse accessed his or her estranged spouse's stored emails and subsequently sought to have them admitted into evidence. The key inquiry in these cases is whether the spouse's actions constituted a violation of New York's eavesdropping statute. If the spouse's actions are a violation of the statute, then the emails are inadmissible evidence.

For example, in *Moore v. Moore*,<sup>124</sup> a wife discovered a laptop in the trunk of her estranged husband's car from which she downloaded Internet messages that she wished to use as evidence in their divorce proceeding.<sup>125</sup> The husband filed a motion to suppress and argued the disk was obtained through violation of New York's eavesdropping statute and was therefore inadmissible.<sup>126</sup> The court rejected this argument and found that accessing files downloaded and saved to a computer did not constitute "intercepting or accessing" a communication in violation of Penal Law § 250.05.<sup>127</sup>

Similarly, in another divorce proceeding, *Boudakian v. Boudakian*,<sup>128</sup> which was decided a few months after *Moore*, a wife downloaded communications from her estranged husband's computer at their home.<sup>129</sup> The court, following *Moore*, also held that the wife did not violate New York's eavesdropping statute because the communications were not in-transit when she accessed them.<sup>130</sup>

The most recent and in-depth discussion of New York's eavesdropping statute was in *Gurevich v. Gurevich*.<sup>131</sup> *Gurevich* was a matrimonial action where the wife gained access to her estranged husband's email account and purported to use those emails to demonstrate that her husband was shielding income from her.<sup>132</sup> The

---

868 (Sup. Ct. 2013) (holding that "pinging" the defendant's cell phone did not violate his Fourth Amendment rights).

123. See *Gurevich*, 886 N.Y.S.2d 558 (Sup. Ct. 2009); *Boudakian*, N.Y. L.J., Dec. 26, 2008 (Sup. Ct. 2008); *Moore*, N.Y. L.J., Aug. 14, 2008 (Sup. Ct. 2008).

124. N.Y. L.J., Aug. 14, 2008 (Sup. Ct. 2008).

125. *Id.*

126. *Id.*

127. *Id.*

128. N.Y. L.J., Dec. 26, 2008 (Sup. Ct. 2008).

129. *Id.*

130. *Id.*

131. *Gurevich v. Gurevich*, 886 N.Y.S.2d 558 (Sup. Ct. 2009).

132. *Id.*

question was whether the emails were inadmissible under N.Y. C.P.L.R. § 4506,<sup>133</sup> which provides:

The contents of any overheard or recorded communication, conversation or discussion, or evidence derived therefrom, which has been obtained by conduct constituting the crime of eavesdropping, as defined by section 250.05 of the penal law may not be received in evidence in any trial, hearing or proceeding before any court . . . .<sup>134</sup>

In other words, the court had to determine whether the wife violated the eavesdropping statute when she accessed her estranged husband's stored emails.<sup>135</sup> First, the court had to analyze the definitions set out in the eavesdropping law, including the definition for "intercept or access."<sup>136</sup>

The court concluded based on the statute's legislative history<sup>137</sup> that the purpose of the statute was to prohibit individuals from intercepting communications that were in-transit.<sup>138</sup> Therefore, the wife did not "intercept" her husband's emails within the meaning of the eavesdropping statute, and N.Y. C.P.L.R. § 4506 did not prevent the emails' admission into evidence.<sup>139</sup> That is, the court concluded that despite the plain language of the statute, New York's eavesdropping law mirrors federal law in that it applies only to those electronic communications that are in-transit and does not apply to those communications that are stored.<sup>140</sup>

As these cases demonstrate, there is a conflict between the plain language of the eavesdropping statute and the courts' recent interpretation. The plain language indicates that *all* electronic communications are covered by New York's eavesdropping law, meaning law enforcement officials must obtain an eavesdropping warrant in order to intercept messages that are both in-transit and stored. Nevertheless, New York courts have interpreted the statute to mirror the federal framework despite its language, meaning that communications that are in-transit require an eavesdropping warrant while those messages that have been received and/or are being stored do not. This conflict begs the critical question, which interpretation is

---

133. *Id.*

134. *See* N.Y. CRIM. PROC. LAW § 4506(1) (McKinney 2013).

135. *See Gurevich*, 886 N.Y.S.2d at 560.

136. *See id.*

137. *See* 1988 N.Y. Sess. Laws 744 (McKinney).

138. *See Gurevich*, 886 N.Y.S.2d at 560–61.

139. *See id.* at 561–62.

140. *Compare Gurevich*, 886 N.Y.S.2d 558, *with* 18 U.S.C. § 2701 (2012).



correct? This Note argues that the New York legislature should revise New York's eavesdropping law to clarify the courts' interpretation.

### III. NEW YORK LAW SHOULD REQUIRE AN EAVESDROPPING WARRANT FOR LAW ENFORCEMENT'S ACCESS TO ALL STORED ELECTRONIC COMMUNICATIONS

The conflict in New York between the plain language of the eavesdropping statute and New York courts' interpretation of the statute creates the opportunity to revise and clarify that statute. This Part proposes a revision to New York's eavesdropping statute to exclude stored electronic communications. It also proposes that New York enact a new law requiring law enforcement officials to procure a search warrant to gain access to stored electronic communications.<sup>141</sup>

Part III.A argues that stored electronic communications should not be protected under New York's eavesdropping statute. This argument is rather simple and straightforward: there must be a balance between the risk to individual privacy rights and the interests of law enforcement counsel against requiring an eavesdropping warrant for stored electronic communications.

Part III.B, however, makes the more contentious argument that stored electronic communications should require law enforcement officials to obtain a search warrant. While the courts have largely shied away from the question—whether the Fourth Amendment protects stored electronic communications—an examination under the reasonable expectation test as set out in *Katz* dictates that a warrant should be required to access these communications. This result, balanced against the interests of law enforcement, supports the conclusion that stored electronic communications should be protected by a warrant requirement in New York.

#### A. Law Enforcement Access to Stored Communications in New York Should Not Require an Eavesdropping Warrant

The weighing of individual privacy rights against law enforcement efficacy counsels against giving stored electronic communications heightened protection under New York's law. The degree of government intrusion upon individuals' privacy does not warrant the

---

141. It is important to note that New York's eavesdropping statute can be revised to exclude stored communications, but must preserve the treatment of in-transit electronic communications due to the requirements under federal law. *See* 18 U.S.C. § 2516(2) (2012).

heightened protection of an eavesdropping warrant. Moreover, requiring law enforcement officials to meet the heightened requirements for an eavesdropping warrant, given this lower risk, will impair their ability to investigate and prosecute crime.

1. *The Threat Posed to Individual Privacy Rights Is Not as Great for Stored Electronic Communications as it Is for in-Transit Electronic Communications*

The differing level of government intrusion between electronic communications that are in-transit and those that are stored supports treating the two types of communications differently.<sup>142</sup> Intercepting electronic communications that are in-transit poses a much greater threat to personal privacy rights than interception of stored electronic communications. Thus, in-transit electronic communications should be given greater protection.

For example, if the government wishes to obtain copies of a stored electronic communication it must first procure the required warrant or court order according to the SCA and serve it on the service provider.<sup>143</sup> Then the provider must turn over the requested communications.<sup>144</sup> Therefore, accessing stored electronic communications is a one-time event. By contrast, if the government instead seeks to intercept electronic communications en route from sender to receiver, they will have to install what is called a “sniffer device”<sup>145</sup> which will monitor *all* communications traveling to and from a given account for a specified period of time. In this way, intercepting in-transit electronic communications is an ongoing process more akin to wiretapping a phone line or bugging a residence.

Accessing stored electronic communications via a compulsory order to service providers represents a lower intrusion upon individual privacy rights and thus should not require the same heightened level of protection as those communications that are in-transit. Wiretapping and other similar methods of intercepting communications while they are en route require law enforcement to make a higher showing upon the understanding that this continuous intrusion poses a great threat to personal privacy rights.<sup>146</sup> The law allows the government to engage in these practices only when they

---

142. See Kerr, *supra* note 62, at 1231.

143. See *supra* Part I.C.

144. See *supra* Part I.C.

145. Kerr, *supra* note 62, at 1231.

146. See *generally* Freiwald, *supra* note 51.

can satisfy the rigorous requirements for an eavesdropping warrant. By contrast, compelling service providers to turn over copies of stored electronic communications does not pose a continuous, extended threat to personal privacy.<sup>147</sup> Instead, law enforcement must make a one-time application for an order and serve it on a service provider.<sup>148</sup>

The lack of continuous intrusion inherent in law enforcement access to stored electronic communications counsels against requiring law enforcement to obtain an eavesdropping warrant under New York's rigorous standards. Additionally, this solution is supported by the disproportionate burden that this standard would place on law enforcement officials.

## *2. Requiring an Eavesdropping Warrant for Access to Stored Electronic Communications Would Overburden Law Enforcement Officials*

Requiring law enforcement officials to obtain an eavesdropping warrant to compel disclosure of stored electronic communications would significantly impede New York officials' criminal investigations. The higher showing required to obtain an eavesdropping warrant could result in delaying access to important evidence and, in some circumstances, preventing access to these communications all together.

For example, the category of courts authorized to issue an eavesdropping warrant is much narrower than those authorized to issue other court orders. Only appellate division and superior court judges and justices can issue an eavesdropping warrant, as opposed to a search warrant, which can be issued by any local criminal court.<sup>149</sup> Additionally, the category of officials authorized to apply for an eavesdropping warrant is also much narrower than those officials that can apply for a search warrant. Only high-level prosecutorial officials of the state may apply for an eavesdropping warrant<sup>150</sup> while any public servant acting in the course of his official duties may apply for a search warrant.<sup>151</sup> When applied to stored electronic communications these procedures could unduly delay government access to key evidence.

---

147. *See generally id.*

148. *See generally id.*

149. *Compare* N.Y. CRIM. PROC. LAW § 700.05(4) (McKinney 2013), *with* N.Y. CRIM. PROC. LAW § 120.30(1) (McKinney 2013).

150. CRIM. PROC. § 700.05(5).

151. *Id.* § 690.05(1).

Additionally, the substantive requirements of an application for an eavesdropping warrant are much more strenuous.<sup>152</sup> To obtain an eavesdropping warrant, an appropriate applicant as defined by the statute must file an application making the following showings: (1) a statement of the applicant's identity and authority to make the application;<sup>153</sup> (2) a statement of the facts that justify the use of the warrant;<sup>154</sup> (3) a statement that the communications are not privileged;<sup>155</sup> (4) a statement that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried;<sup>156</sup> (5) a statement of the period of time for which surveillance is sought;<sup>157</sup> and (6) a statement of any previous applications for surveillance of the same persons or places as are the subject of the current application.<sup>158</sup>

The second requirement for the application, the statement of facts that justify the use of the warrant, must include:

- (i) a statement of facts establishing probable cause to believe that a particular designated offense has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted or the video surveillance is to be conducted, (iii) a particular description of the type of the communications sought to be intercepted or of the observations sought to be made, and (iv) the identity of the person, if known, committing such designated offense and whose communications are to be intercepted or who is to be the subject of the video surveillance.<sup>159</sup>

Requirements (ii) and (iii) above, implement the Fourth Amendment's "particularity" requirement.<sup>160</sup> Importantly, (iii) specifies that the applicant particularly describe *the type of communication sought*. This means that law enforcement agents must include a description of the communication's subject matter so

---

152. See *supra* Part I.D.

153. N.Y. CRIM. PROC. LAW § 700.20(2)(a) (McKinney 2013).

154. CRIM. PROC. § 700.20(2)(b).

155. CRIM. PROC. § 700.20(2)(c).

156. CRIM. PROC. § 700.20(2)(d).

157. CRIM. PROC. § 700.20(2)(e).

158. CRIM. PROC. § 700.20(2)(f).

159. CRIM. PROC. § 700.20(2)(b).

160. See *Berger v. New York*, 388 U.S. 41, 55–56 (1967) (“The Fourth Amendment commands that a warrant issue not only upon probable cause supported by oath or affirmation, but also ‘particularly describing the place to be searched, and the persons or things to be seized.’”).

that they are not given a blank check to intercept all communications sent to a certain account.

This showing is substantially higher than that required for obtaining a search warrant in New York. In New York, the statement of facts justifying the search warrant must simply include a statement that there is probable cause for the search and that the item sought will be found in the place described.<sup>161</sup>

Requiring government officials to make these heightened showings given the lower intrusion on individual privacy is inappropriate. If New York requires its law enforcement officials to first obtain an eavesdropping warrant before they gain access to stored emails, there will necessarily be cases in which the crime charged is not listed as a specified crime under New York's statute.<sup>162</sup> Thus, for those cases, law enforcement officials will not be allowed to access a suspect's stored electronic communications, even if they can satisfy all of the other rigorous requirements.

Additionally, New York's statute (like the federal framework) requires an applicant to demonstrate that normal investigative procedures have been tried and have failed. In New York this requirement does not mean that the applicant needs to show that every other investigative technique has been exhausted,<sup>163</sup> but it does require a showing that other techniques have been tried first or that other techniques would be ineffective. This requirement was implemented as part of the Wiretap Act out of a concern that such an intrusive search should be a last resort.<sup>164</sup> Access to stored electronic communications, however, does not represent the same continuous intrusion that wiretapping, bugging, or installing a sniffer device does. The law should not require that law enforcement officials exhaust other avenues first.

Given the substantial burden that an eavesdropping warrant requirement would place on New York law enforcement and the lower threat to individual privacy rights under those circumstances, reinforcing the plain language of the statute and requiring an eavesdropping warrant for stored electronic communications would

---

161. N.Y. CRIM. PROC. LAW § 690.35(3)(b) (McKinney 2013).

162. For example, enterprise corruption is not a designated offense under New York's statute and therefore eavesdropping warrants will not be issued for these investigations. *See People v. Wakefield Fin. Corp.*, 590 N.Y.S.2d 382, 387 (Sup. Ct. 1992).

163. *See People v. Haji*, 767 N.Y.S.2d 826, 827 (App. Div. 2003).

164. *See United States v. Kahn*, 415 U.S. 143, 153 (1974); *United States v. Giordano*, 416 U.S. 505, 515 (1974).

be inappropriate. Instead, a search warrant requirement would strike the right balance between the interests of law enforcement and the individual privacy interests.

### **B. New York Should Enact a Warrant Requirement for Stored Electronic Communications**

This Part argues that New York should enact a warrant requirement for law enforcement access to stored electronic communications rather than await guidance from the courts or Congress. This conclusion is supported by the application of the “reasonable expectations” test in *Katz*. Moreover, a warrant requirement strikes the appropriate balance between law enforcement efficacy and personal privacy rights. Finally, requiring a search warrant for stored electronic communications would eliminate the outdated distinctions made in the federal framework,<sup>165</sup> providing clear guidance for all parties subject to the law.

#### *1. Reasonable Expectation of Privacy in Electronic Communications*

Any consideration of surveillance law requires an analysis under the Fourth Amendment.<sup>166</sup> The Fourth Amendment requires that when an individual has a “reasonable expectation of privacy”<sup>167</sup> in a certain space, or in this case in certain personal communications, the government must demonstrate probable cause and procure a search warrant before it may conduct any lawful search or seizure.<sup>168</sup> Therefore, it is necessary to consider whether individuals have a reasonable expectation of privacy in stored electronic communications in contemplating whether to implement a search warrant requirement.

---

165. See Bowman, *supra* note 32, at 831.

166. See U.S. CONST. amend. IV. (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

167. In *Katz v. United States*, 389 U.S. 347 (1967), Justice Harlan wrote that there is a two-part inquiry in determining whether an individual has a reasonable expectation of privacy. First, one must ask whether the individual’s conduct reflects a subjective expectation of privacy. If the individual is found to have this subjective expectation then the second inquiry is objective whether the actual expectation one that society as a whole recognizes. See *id.* at 361 (Harlan, J., concurring).

168. See *id.* at 362.

In *Katz v. United States*, Justice Harlan set out a two-part test to determine whether the Fourth Amendment requires law enforcement officials to procure a search warrant before a search or seizure.<sup>169</sup> The first part asks whether the individual has an actual expectation of privacy in this space or property. This inquiry is subjective. The second part is an objective inquiry. It asks whether that expectation is one that society finds reasonable.<sup>170</sup> This Note asserts that individuals enjoy a reasonable expectation of privacy in stored electronic communications; thus, New York State should require law enforcement officials to procure a search warrant before accessing those communications.

In supporting that argument, this Subpart first discusses why the third-party doctrine does not defeat the reasonable expectation test as applied to stored electronic communications. Next, this Subpart applies the *Katz* test to electronic communications. Specifically, it explores the extent to which the reliance upon and pervasiveness of electronic communications in today's society supports the conclusion that society has an objectively reasonable expectation of privacy in these communications.

*a. The Third-Party Doctrine Should Not Defeat Fourth Amendment Protection of Stored Electronic Communications*

The third-party doctrine is a central tenet of Fourth Amendment jurisprudence. The doctrine holds that when an individual surrenders an item (or in this case, a communication) to a third party, he forfeits all Fourth Amendment rights in that information or communication.<sup>171</sup> In other words, the Supreme Court has found that a person cannot have a reasonable expectation of privacy in information he relates to a third-party.<sup>172</sup> The argument applying the third-party doctrine to stored electronic communications relies on the transmission through, and storage of, these messages with third-party service providers like ISPs and SMCs as discussed in Part I.

However, the nature of electronic communications makes the application of the third-party doctrine to completely defeat Fourth Amendment protection of electronic communications

---

169. *Id.* at 361.

170. *Id.* at 361–62.

171. *See* *Smith v. Maryland*, 442 U.S. 735, 744 (1979); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

172. *See* Kerr, *supra* note 171, at 563; *see also* *Smith*, 442 U.S. at 744; *United States v. Miller*, 425 U.S. 435, 443 (1976).

inappropriate.<sup>173</sup> To begin, the third-party doctrine has traditionally been used to defeat protection of “business records.”<sup>174</sup> In a series of cases, the Supreme Court has held that records of individuals’ transactions maintained by third-party business entities (like bank or tax records) are not protected under the Fourth Amendment.<sup>175</sup> But electronic communications are nothing like business records; they are private communications. Thus, applying the third-party doctrine to defeat Fourth Amendment protection of these communications would be inconsistent with the doctrine’s past application.<sup>176</sup> The contents of business records are turned over with the understanding that the third party will need to review the contents of those records in the course of its business activities. On the other hand, the use of web-based email or cellular text messaging services does not accompany the understanding that the service provider will need to access the communications content.

The larger point, however, is that the third-party doctrine is simply not compatible with the methods of modern communication. One of the rationales of the doctrine’s application has been that individuals have voluntarily assumed the risk that the third-party will disclose that information.<sup>177</sup> In the context of stored electronic communications, however, it is very uncertain—in fact highly doubtful—that writing an email or composing a text-message means that a user is voluntarily assuming the risk that an ISP or cell phone service will turn the content of those messages over to the government.<sup>178</sup>

---

173. This conclusion is supported by many privacy scholars. See Bellia & Freiwald, *supra* note 31, at 148; Kerr, *supra* note 171, at 563; see also Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference*, 74 *FORDHAM L. REV.* 747, 753 (2005).

174. *Miller*, 425 U.S. at 441–43 (holding that the disclosure of records to a bank defeats Fourth Amendment protection); *Couch v. United States*, 409 U.S. 322, 335 (1973) (holding that there is no expectation of privacy where records are turned over to an accountant); see Bellia & Freiwald, *supra* note 31, at 145; see also Mulligan, *supra* note 31, at 1576–82. The “business records” cases include *Couch v. United States*, *United States v. Miller*, and *Smith v. Maryland*. See *Smith*, 442 U.S. at 742 (holding that individuals have no expectation of privacy in the phone numbers they dial because they know this information will be conveyed to the phone company).

175. See Mulligan, *supra* note 31, at 1562.

176. See Bellia & Freiwald, *supra* note 31, at 148–49 (noting that emails, unlike business records, entail private communications); Mulligan, *supra* note 31, at 1581–82.

177. See *Miller*, 425 U.S. at 443 (“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”).

178. See Bellia & Freiwald, *supra* note 31, at 148–49, 153–56.



This point is reinforced by the fact that when the ECPA was passed in 1986, electronic communications worked much differently than they do today. Communicating via email in the 1980s involved downloading email messages from a server to a home computer.<sup>179</sup> If law enforcement officials wished to access those stored messages, they would have to access them through the individual's home computer, which would require a search warrant. Because this was the dominant email system at the time, the SCA's distinctions were arguably drafted with this method in mind; in other words, almost all email systems were considered ECS providers—they would transmit the message from sender to receiver, storing the message intermediately along the way.<sup>180</sup> Additionally, Congress created the category for RCS providers largely in light of the third-party doctrine. At the time, the services of third-party service providers that offered sophisticated remote storage were prohibitively expensive.<sup>181</sup> Thus, remote storage was a service offered to large businesses that needed space to store their data. In this way, the services of RCS providers in the 1980s resemble the “business records” cases.

The distinction the SCA makes between ECS and RCS providers is not as clear now as it once was in 1986. Today, web-based email providers like Gmail store all of their users' messages in remote storage, and in intermediate storage during transmission. In effect, large businesses are no longer the only users of remote storage. Instead most users of web-based email (and users of text-messages) have their messages stored in remote storage.<sup>182</sup> Therefore, while application of the third-party doctrine may have comported with the doctrine's past in 1986 when the ECPA was enacted, the advances in electronic communications technology since then casts serious doubt on its application to stored electronic communications today.

Even Supreme Court justices have recently expressed disapproval of application of the third-party doctrine to modern technology. In her concurrence in *United States v. Jones*,<sup>183</sup> Justice Sotomayor stated,

---

179. *See supra* Part I.B.

180. *See* Robison, *supra* note 8, at 1205–06.

181. *See id.* at 1206–07.

182. *See generally id.*

183. *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (holding that the government's installation of a Global Positioning System tracking device on a target's vehicle to obtain information was a violation of the defendant's Fourth Amendment rights.)

[I]t may be necessary to reconsider the premises that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.<sup>184</sup>

For these reasons, the third-party doctrine should not defeat the reasonable expectation of privacy in stored electronic communications.

*b. Society Has an Objectively Reasonable Expectation of Privacy in Stored Electronic Communications*

Under the two-prong test set out in Justice Harlan's concurrence in *Katz*, the compelled disclosure of stored electronic communications should require law enforcement officials to procure a search warrant. While the outcome under the subjective prong is case-dependent, the analysis under the test's objective prong dictates that access to stored electronic communications should require a search warrant under the Fourth Amendment.

The subjective prong of the *Katz* test's application is not predictable because it is necessarily a case specific inquiry, although most individuals, if asked whether they expect that strangers would read their email or text messages, would probably respond that they do not. As to the second prong of the *Katz* test, in considering whether there is an objective expectation of privacy in stored electronic communications, a court must ask what society is entitled to believe, even if society might perceive a certain mode of communication as less than secure.<sup>185</sup>

Under the objective inquiry set out in *Katz*, it is important to consider the growing role that electronic communications like text messages and email messages play in society today.<sup>186</sup> One way to evaluate whether society has an objective expectation of privacy in stored electronic communications is through surveys.

One recent study found that young adults are as likely to connect with others electronically as they are in person.<sup>187</sup> This study shows that young adults today make a total of seventy-four electronic

---

184. *Id.* at 957 (citations omitted).

185. *See* Bellia & Freiwald, *supra* note 31, at 137–38.

186. *See id.* at 138–39.

187. *See generally* MILLER, *supra* note 10.

contacts a month.<sup>188</sup> The report compares the average electronic contacts by young adults to personal contact with individuals and concluded that the general trend is that young adults tend to communicate via electronic networks just as often as they do in person.<sup>189</sup> This survey demonstrates that electronic communications like texts and emails are beginning to replace traditional modes of communications that already enjoy Fourth Amendment protection.

Similarly, another 2011 study found that 83% of American adults own cell phones and 73% of them send and receive text messages.<sup>190</sup> Moreover, 31% of text message users stated that they preferred to be contacted via text messaging instead of talking on the phone.<sup>191</sup>

Perhaps most importantly, another recent study found that 68% of adult Internet users say it is very important to them that no one, other than those authorized to, have access to the content of their email.<sup>192</sup> Additionally, the study found that 62% of adult Internet users say it is very important to them that only the people with whom they exchange emails have access to them.<sup>193</sup> This survey demonstrates that despite the potential understanding that electronic communications are less secure, society still holds the belief that these communications should be private.

These studies and statistics demonstrate the prevalence of and reliance on electronic communications in our modern world. This factor is important in determining the objective inquiry of the “reasonable expectations” test because it demonstrates normative reliance on electronic communications showing that society is entitled to believe that these communications are private.<sup>194</sup> This data is also significant in that it tends to demonstrate that email (and to a lesser extent text-messages) has replaced, to a certain degree, traditional communications that courts have already determined carry a “reasonable expectation of privacy.”<sup>195</sup> The fact that electronic

---

188. *See id.* The term “electronic contacts” includes non-work emails, Facebook visits, tweets, Skype visits, and the transmission of digital pictures. Additionally, email messages accounted for over half of the seventy-four electronic contacts. *Id.*

189. *See id.* fig.1.

190. PEW RESEARCH CTR., *supra* note 11, at 1.

191. *Id.*

192. PEW RESEARCH CTR., ANONYMITY, PRIVACY, AND SECURITY ONLINE 19 (2013).

193. *Id.*

194. *See* Bellia & Freiwald, *supra* note 31, at 138–39. *See also* Mulligan, *supra* note 31, at 1571–76.

195. *See* Bellia & Freiwald, *supra* note 31, at 138–39; *see also* Katz v. United States, 389 U.S. 347, 352, 360 (1967) (holding that there is a reasonable expectation of privacy in conversations occurring over telephone); Silverman v. United States, 365

communications have begun to replace these traditional forms of communication suggests that society holds a belief in privacy in electronic communications similar to the belief in the privacy of traditional modes of communication.<sup>196</sup>

Under the *Katz* test, society has a reasonable expectation of privacy in electronic communications and law enforcement access to these communications should at least require a search warrant. This conclusion is supported by significant scholarship<sup>197</sup> and at least one court decision.<sup>198</sup>

## 2. *Requiring a Search Warrant Will Not Over-Burden Law Enforcement Officials*

Requiring a search warrant under New York law for all stored electronic communications would make it more difficult for law enforcement to access certain types of stored electronic communications. The current requirements are so weak, however, that a search warrant will not overburden law enforcement and would in fact be proportionate to the privacy interests at stake. Under the current federal framework certain types of stored electronic communications only require a subpoena or court order for the government to access those communications.<sup>199</sup> If New York eliminates this distinction and replaces it with a warrant requirement for all stored electronic communications, state law enforcement agents would have to make a greater showing than they once did to obtain stored electronic communications like emails and text messages. The Department of Justice (DOJ), however, has recently made statements that disapprove of the effectiveness of the

---

U.S. 505, 510 (1961) (holding that the interception of telephonic and in-person conversations is a search under the Fourth Amendment).

196. See generally Bellia & Freiwald, *supra* note 31.

197. See generally sources cited *supra* note 31.

198. The Sixth Circuit recently held that there is a reasonable expectation of privacy in emails and that government officials violate the Fourth Amendment when they obtain emails without first obtaining a search warrant. See *United States v. Warshak*, 631 F.3d 266 (2010).

199. 18 U.S.C. § 2703 (2012). For example, emails and text-messages that have been “stored” for more than 180 days only require that the government obtain a subpoena to access them. § 2703(b). See *ECPA (Part I): Lawful Access to Stored Content Before the Subcomm. on Crime, Terrorism, Homeland Security, & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 3 (2013) (statements of Rep. Scott) (“[A] warrant is required to access the content of e-mails while it waits in electronic communications service storage to be read by the recipient, the instant the e-mail is opened by the recipient, it may lose that high standard of protection and become accessible by subpoena rather than by a warrant.”).

distinctions created under the SCA in the face of modern modes of communication.<sup>200</sup> In fact, the DOJ has also admitted recently that the argument for requiring law enforcement to obtain a warrant based on probable cause to compel disclosure of the contents of stored e-mails “has considerable merit.”<sup>201</sup>

3. *Requiring a Search Warrant for Access to Stored Electronic Communications Would Eliminate Confusion Over the Distinctions Contained in the SCA and Pressure Congress to Take Action*

Two additional benefits to a warrant requirement for stored electronic communications bear discussion. First, requiring a search warrant for government access to stored electronic communications in New York would eliminate all of the confusion created by the SCA. A blanket search warrant requirement would mean that both law enforcement officials and electronic communication users will have a clear understanding of the law. The distinctions made as to how long a message has been in storage or what type of communication provider holds the message will no longer exist. Instead, the sole inquiry when government officials seek stored emails or texts from a service provider would be whether the government has demonstrated probable cause.

While this clarity would certainly benefit the users of stored electronic communications, it may benefit service providers even more.<sup>202</sup> Under the SCA, service providers are often placed in difficult positions. They have the choice to either protect their users’ data (potentially facing obstruction of justice charges by refusing to cooperate with investigators), or cooperate with subpoenas and court orders and face losses to their business when users learn that their communications are not secure. Since the SCA is an elaborate and confusing framework and the courts have provided little guidance, service providers often have to guess at which action will limit their

---

200. In her testimony at the Hearing Before the Subcommittee on Crime, Terrorism, Homeland Security and Investigations of the Committee on the Judiciary, Elana Tyrangiel, acting Assistant Attorney General, stated, “[The Department of Justice] agree[s], for example, that there is no principal basis to treat e-mail less than 180 days old differently than e-mail more than 180 days old.” *ECPA (Part I): Lawful Access to Stored Content Before the Subcomm. on Crime, Terrorism, Homeland Security, & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 14 (2013).

201. *See id.*

202. For more on the tech industry’s reaction to revelations of government surveillance, see Claire Cain Miller, *Angry Over U.S. Surveillance, Tech Giants Bolster Defenses*, N.Y. TIMES, Oct. 31, 2013, [http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html?\\_r=1&](http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html?_r=1&).

losses. Under a search warrant requirement, ISPs and SMCs who provide services to users in New York would clearly understand those situations when disclosure is compelled and those situations where they must protect their users. In other words, this clarity would allow service providers to predict outcomes and adjust their behavior accordingly.

A blanket search warrant requirement would also allow the law to be more flexible and adapt to rapidly changing technologies. The SCA drafters arguably drew on the technology that existed then to create the current surveillance framework.<sup>203</sup> In effect, the SCA is full of distinctions that may have made sense at the law's inception, but no longer fit in with today's modern modes of electronic communication. A search warrant requirement, devoid of any minute distinctions, would simply hold that government access to any and all stored electronic communications would require a search warrant. As technology changes and evolves the question will become whether a given message is a "stored electronic communication." This question can be resolved by courts and will not require legislatures to revise the law every time that society advances.

Finally, if New York implements a blanket search warrant requirement for government access to New Yorkers' emails and text messages, it is possible that Congress would be pressured to do the same on the federal level. New York may serve as an example of how such an amendment would work and perhaps relieve uncertainty for Congress. Moreover, the more states that take action the harder it becomes for Congress to ignore. Since the Snowden scandal, over two-dozen privacy laws have been passed in more than ten states.<sup>204</sup> These new laws range from laws limiting how schools can collect their student's data to determining whether police must procure a warrant in order to use cell-site location data.<sup>205</sup>

#### IV. THE PROPOSED REVISION

The difference between the plain language of the statute and the New York courts' interpretation of the statute gives New York the perfect opportunity to clarify the law. In addition, New York's strong

---

203. *See supra* Part I.B.

204. *See* Somni Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES, Oct. 30, 2013, <http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html>.

205. *See id.*

history of protecting its citizens' privacy<sup>206</sup> makes it the optimal state to blaze the trail (along with Texas) in protecting Americans from government surveillance of their stored electronic communications.

The following proposals would clarify that New York government officials do not need to obtain an eavesdropping warrant to access New Yorker's stored electronic communications. However, this Note also proposes changes that would require New York officials to obtain a search warrant upon a showing of probable cause in order to access these communications.

#### A. Changes to the Language of New York Penal Law Section 250.00 and New York Criminal Procedure Law Section 700.05

The proposed revision to the New York eavesdropping law could be effected very easily. New York's penal law<sup>207</sup> currently provides the definition of "intercepting or accessing of an electronic communication" as follows:

"Intercepting or accessing of an electronic communication" and "intentionally intercepted or accessed" means the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of the sender or intended receiver thereof, by means of any instrument, device or equipment, except when used by a telephone company in the ordinary course of its business or when necessary to protect the rights or property of such company."<sup>208</sup>

The following represents the proposed changes that could be made to the language of the statute to give it the desired effect:

~~"Intercepting or accessing of an electronic communication"~~ and ~~"intentionally intercepted or accessed"~~ means the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, **while the communication is between the point of origin and the point of reception and** without the

206. New York courts have declined to implement doctrines in the field of search and seizure that have been adopted by other states because these doctrines intrude too greatly on personal privacy. *See People v. Diaz*, 612 N.E.2d 298 (N.Y. 1993) (rejecting the "plain touch" doctrine for so-called *Terry* searches for weapons in part because the intrusion upon personal privacy is too great); *see also People v. Torres*, 543 N.E.2d 61 (N.Y. 1989) (holding that police officers need more than reasonable suspicion to search the inside of a vehicle for weapons).

207. It is important to note that amending this definition in the penal law would also affect the criminal prohibition on eavesdropping, criminalizing only the interception of in-transit electronic communication under section 250 of the New York Penal Law. N.Y. PENAL LAW § 250.00 (McKinney 2013).

208. PENAL LAW § 250.00(6).

consent of the sender or intended receiver thereof, by means of any instrument, device or equipment, except when used by a telephone company in the ordinary course of its business or when necessary to protect the rights or property of such company.”

Additionally, the definition of “eavesdropping” contained in section 700.05 of the New York Criminal Procedure Law would also need to be revised slightly to make the two statutes compatible. The statute currently reads as follows:

“Eavesdropping” means “wiretapping”, “mechanical overhearing of conversation” or the “intercepting or accessing of an electronic communication” . . . .

The following represents the changes to this definition:

“Eavesdropping” means “wiretapping”, “mechanical overhearing of conversation” or the “intercepting ~~or accessing~~ of an electronic communication” . . . .

These revisions would put the proposed solution into effect, clarifying that New York’s eavesdropping law does not require an eavesdropping warrant for law enforcement access to stored electronic communications. The statute’s language could also be revised in a few other minor respects are beyond the scope of this Note.<sup>209</sup>

These revisions are not likely to be controversial. No courts have held that stored electronic communications require an eavesdropping warrant.<sup>210</sup> In fact, courts considering the question have found that

---

209. This author would also recommend a few other alterations to the statute that would simply modernize the language to bring it up to speed with current technology. For example, one change that may be helpful would be to eliminate the term “telephonic or telegraphic communication” and replace it with the federal law equivalent, “wire communication.” Compare N.Y. CRIM. PROC. LAW § 700.05 (McKinney 2013), and PENAL LAW § 250.00(3), with 18 U.S.C. § 2510(1) (2012). In fact, an amendment made to the law shortly after the ECPA was passed confusingly uses the term “wire communication,” even though that term is not defined anywhere in New York’s statute. See CRIM. PROC. § 700.05(4). However, this revision will not be without practical effect. If New York adopts the ECPA’s language here and replaces the term “telephonic or telegraphic communication” with “wire communication” that will mean that stored voicemail messages will be excluded from the eavesdropping statute as well. This Note would argue that this exclusion is appropriate for all of the reasons why other stored electronic communications should be excluded from New York’s eavesdropping statute. Therefore, the phrase “such term includes any electronic storage of such communications” contained in New York Penal Law section 250.00(3) should also be eliminated since that language is meant to expressly include voicemail in the definition of “telephonic communication.”

210. See *supra* Part II.



New York's statute mirrors the federal law.<sup>211</sup> In effect, this revision would simply bring New York's statute into line with the Wiretap Act, clarifying that law enforcement officials are only required to obtain an eavesdropping warrant for in-transit communications. It may seem from the language proposed to be omitted from the statute that the revision will take away certain protections, but in reality it will simply codify the law as it already exists in the courts.

### **B. Proposed Statute Requiring a Search Warrant for Law Enforcement Access to Stored Electronic Communications**

In considering how to implement a warrant requirement in the state of New York, this Note has the advantage of a recent example. Texas Governor Rick Perry signed a bill requiring a search warrant for state law enforcement access to any and all stored email messages in the state of Texas on June 14, 2013.<sup>212</sup> The new law<sup>213</sup> revised various provisions of the criminal procedure code to implement the changes.<sup>214</sup> Specifically, the bill revised Texas's statute governing the issuance of search warrants to add the following language:

(a) A search warrant may be issued to search for and seize:

...

(13) electronic customer data held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage.

(b) For purposes of Subsection (a)(13), "electronic communication," "electronic storage," and "wire communication" have the meaning assigned by Article 18.20, and "electronic customer data" has the meaning assigned by Article 18.21.<sup>215</sup>

Additionally, the Texas legislature amended the definition of "electronic storage"<sup>216</sup> to read:

---

211. See generally *People v. Harris*, 949 N.Y.S.2d 590 (Crim. Ct. 2012); *Gurevich v. Gurevich*, 886 N.Y.S.2d 558 (Sup. Ct. 2009); *Boudakian v. Boudakian*, N.Y. L.J. Dec. 26, 2008 (Sup. Ct. 2008); *Moore v. Moore*, N.Y. L.J. Aug. 14, 2008 (Sup. Ct. 2008).

212. See *Bill: HB 2268*, TEX. LEGISLATURE ONLINE, <http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB2268> (last visited Mar. 15, 2015). See generally *Sullivan*, *supra* note 19.

213. See TEX. CODE CRIM. PROC. ANN. art. 18.02 (West 2013).

214. See H.B. 2268, 83rd Leg. (Tex. 2013). Specifically, the bill revised articles 18.02, 18.06–07, and 18.20–21 of Texas's Code of Criminal Procedure.

215. TEX. CODE CRIM. PROC. ANN. art. 18.02 (West 2013).

216. TEX. CODE CRIM. PROC. ANN. art. 18.20(20) (West 2013).

“Electronic storage” means any storage of electronic customer data in a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion or transmission and includes any storage of a wire or electronic communication by an electronic communications service or a remote computing service.<sup>217</sup>

The effects of these changes is to make clear that a search warrant is required for government access to any and all stored electronic communications.<sup>218</sup> The changes to the definition of “electronic storage” would clarify that a search warrant is required regardless of whether or not the message is being temporarily stored or permanently stored and regardless of whether the message is stored with an ECS or an RCS. In so doing, Texas has eliminated the distinctions created under the SCA. In Texas, law enforcement officials are required to obtain a search warrant for messages that are temporarily stored on their way to the recipient. Law enforcement will also need a warrant to access unopened emails and text messages. Texas government officials are even required to obtain a warrant before reading messages that have been read and remain in storage with service providers’ servers for long periods of time.

Texas also included a provision stating that a search warrant for electronic communications could be issued regardless of where the customer data was held, whether it was within Texas or another state.<sup>219</sup>

Similarly, the New York legislature could also revise the law to make it clear that a warrant is required for the search of stored electronic communications. But revising New York’s law may require more extensive amendments. For example, the term “electronic storage” does not appear at all in section 700 of New York’s criminal procedure law and while the term appears in section 250 of the penal law, it is not defined.<sup>220</sup> Therefore, simply adding “access to stored electronic communications” to the list of evidence that require search warrants would not be sufficient since under New York’s current law

---

217. *Id.*

218. In Texas, stored electronic communications also include stored voicemail messages. Therefore, for access to these stored voicemail messages, law enforcement officials must obtain a search warrant. *See* TEX. CODE CRIM. PROC. ANN. art. 18.20(20) (including in the definition of “electronic storage” “storage of a wire . . . communication by an electronic communications service or a remote computing service.”)

219. *See* TEX. CODE CRIM. PROC. ANN. art. 18.21(5)(a).

220. *See* N.Y. PENAL LAW § 250.00 (McKinney 2013); N.Y. CRIM. PROC. LAW § 700.05 (McKinney 2013).

it is unclear what stored electronic communications are. Regardless of how the amendment to New York law is formed, a definition of “electronic storage” in section 250, section 700 or elsewhere is necessary.

Notice is another issue to consider. Recently, California’s legislature approved a bill<sup>221</sup> that was very similar to Texas’s amendment. It would have required law enforcement officials in California to obtain a search warrant prior to accessing stored electronic communications like emails and text messages.<sup>222</sup> Unlike Texas, California’s bill would have required state law enforcement to notify email account holders that a search of their account had taken place.<sup>223</sup> Due to these heightened notice requirements, California Governor Jerry Brown vetoed the bill.<sup>224</sup> Under the SCA, one advantage to law enforcement officials is that if they obtain a search warrant for access to stored electronic communications, they do not have to notify the suspect.<sup>225</sup> Requiring that law enforcement officials first obtain a search warrant and then notify the suspect would perhaps overburden them, disrupting the balance struck by a warrant requirement. In considering a revision to its surveillance statute, the New York legislature should assess whether a notice requirement would tip the scale too far in favor of personal privacy interests and too far against government interests.

Overall, a blanket search warrant requirement would solve many of the problems and eliminate much of the inherent confusion under New York’s current domestic surveillance law. While an amendment would not protect New Yorkers from surveillance by federal officials,<sup>226</sup> it would ensure that New Yorkers’ emails and text messages are not accessed without probable cause by state law enforcement officials and may have the added bonus of providing pressure on Congress to take action.

---

221. See S.B. 467, 2013–2014 Sess. (Cal. 2013).

222. See Jaikumar Vijayan, *Calif. Governor Vetoes Email Privacy Legislation for Third Time*, COMPUTERWORLD (Oct. 15, 2013), [http://www.computerworld.com/s/article/9243227/Calif.\\_governor\\_vetoes\\_email\\_privacy\\_legislation\\_for\\_third\\_time](http://www.computerworld.com/s/article/9243227/Calif._governor_vetoes_email_privacy_legislation_for_third_time).

223. See *id.*

224. See Letter from Edmund G. Brown, Governor of California, to State Senate (Oct. 12, 2013) (“The bill, however, imposes new notice requirements that go beyond those required by federal law and could impede ongoing criminal investigations. I do not think that is wise.”).

225. See 18 U.S.C. § 2703 (2012).

226. See 18 U.S.C. § 2516(a) (2012) (specifying that the ECPA governs the interception of communications by the Federal Bureau of Investigation or other federal agency).

### CONCLUSION

Americans have outgrown the nation's surveillance laws. The current federal framework does not adequately protect electronic messages in light of the growing prevalence of these modes of communication. Change is necessary. Given the delay in legislation at the federal level, states should take action to protect their citizens. The current conflict between the plain language of the eavesdropping statute in New York and the recent interpretations of that statute by the courts presents the New York legislature with the opportunity to amend its statute and provide its citizens with greater protection from government surveillance. In so doing, New York will not only afford its citizens better protection from state government surveillance but will also apply pressure to lawmakers on the federal level.

Excluding stored electronic communications from New York's surveillance statute and implementing a search warrant requirement for these communications strikes the appropriate balance between individual privacy interests and law enforcement efficacy. This amendment will ensure that the emails and text messages of innocent New Yorkers—like Amy, Joe, and Michael, described above—will be safe from prying government eyes. However, New York officials can still gain access to the emails and text messages of New Yorkers in the course of their investigations upon a showing of probable cause.