Chicago-Kent Law Review

Volume 95
Issue 3 *Reviving the American Jury*

Article 7

4-27-2021

DISCUSSING PRIVACY IN SEC SUBPOENA PRACTICE AFTER CARPENTER V. UNITED STATES

William A. Ballentine
Chicago-Kent College of Law

DISCUSSING PRIVACY IN SEC SUBPOENA PRACTICE AFTER *CARPENTER V. UNITED STATES*

WILLIAM A. BALLENTINE*

INTRODUCTION

Imagine the Securities and Exchange Commission ("SEC") has initiated a formal investigation into a hedge fund after suspecting several key officers of insider trading and conducting a thorough examination. One of the fund executives receives a subpoena ordering all the documents in her office "related to the investigation" be turned over to the SEC, including her emails, chat room conversations, travel records, expense reports, and any other business-related communications. Although firm policy requires written work-related communications to be done only through company email or Bloomberg chat, the executive is concerned that her personal smart phone may be implicated in the subpoena as well. Many of her fellow colleagues are also her friends, so naturally she uses her smart phone for both personal and work-related reasons.

This Note discusses what effects, if any, the decision handed down in *Carpenter v. United States* may have on national subpoena practice, focusing solely on the Securities and Exchange Commission as the agency generally enjoys broad authority to issue subpoenas. Part I explains the background leading up to *Carpenter* and its highly anticipated holdings about statutorily mandated production being unable to endure Fourth Amendment scrutiny. An analysis of three different ways to acquire information in a government investigation—through a warrant, grand jury subpoena, or the Stored Communications Act in certain circumstances—takes place in Part II. Part III then discusses the general standard for administrative subpoenas as a fourth method of obtaining information. As a method requiring less of a showing than the Stored Communications Act, this Note will argue that issuing an administrative subpoena for personal documents would not likely withstand a Fourth Amendment challenge as seen in *Carpenter*. Part IV discusses troubling scenarios where the SEC could demand

* Chicago-Kent College of Law, *Juris Doctor Candidate*, May 2020. I would like to thank Professor Doug Godfrey for his inspiration and guidance throughout writing this Note.

private documents, along with what a Fourth Amendment challenge to an SEC subpoena may sound like after *Carpenter*. Finally, Part V makes concluding comments about subpoena practice and privacy in a modern world.

I. CARPENTER V. UNITED STATES

Carpenter is a highly anticipated Supreme Court case concerning the privacy of an individual's historical cell phone location records stored with a wireless carrier. The decision was handed down in June 2018. In delivering the opinion of the Court, Chief Justice Roberts emphasized how pervasive cell phone usage has become in modern American society and, thus, expressed concern over colliding technological advancements and civil liberties. Certainly, Americans have become accustomed to cell phones being an integral part of everyday life. Approximately 94% of American adults in modern society use cell phones for various functions and pleasures, especially considering the seemingly endless capabilities of the popular smartphone.[1] Cell phones enable people to be readily available and follow people everywhere they go—even to the most intimate spaces. While there is no doubt cell phones provide an ease to certain aspects of life, the technology also inherently requires anyone with a cell phone to sacrifice some of their privacy.

To perform properly, cell phones must connect to radio antennas called "cell-sites" which are found in a variety of places, such as towers or light posts.[2] Modern devices are constantly scanning the surrounding area for a signal—sometimes multiple times a minute—even when the cell phone's owner is not actively using the phone's features.[3] In effect, cell phones are continuously relaying their approximate location to cell towers and, thus, the user's cell service provider. The accuracy of the cell phone's location directly depends on the concentration of the cell-sites in a given area, so populated urban areas are seeing increasingly compact coverage as more cell-sites are installed there.[4]

This geographic data is properly referred to as an individual's cell-site location information (CSLI), which are time-stamped records created every time a cell phone connects to a cell-site.[5] Cell phone service providers reg-

1. KYLE TAYLOR & LAURA SILVER, PEW RESEARCH CTR., SMARTPHONE OWNERSHIP IS GROWING RAPIDLY AROUND THE WORLD, BUT NOT ALWAYS EQUALLY (2019), http://www.pewglobal.org/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ [https://perma.cc/V43S-V8H5].

2. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

3. *Id.*

4. *Id.* at 2211–12.

5. *Id.* at 2211.

ularly collect this data for performance and billing purposes.[6] Law enforcement may access this data as it happens in real time by asking the court for a prospective order, or it may access the data already retained by the service provider to get a better sense of a suspect's past whereabouts.[7] In both instances, law enforcement must apply for a court order to access the data.[8]

Law enforcement can request both historical and prospective CSLI through administrative processes in order to put together a sequence of past events or to ascertain the location of an individual during a past crime.[9] In *Carpenter*, the Government sought to do just that by relying on a statutory regime, namely the Stored Communications Act (SCA), to gain access to a criminal suspect's historical location information through the suspect's cell service provider.[10]

A. Background

The United States Government suspected that Timothy Carpenter, the petitioner in this case, played a role in a series of robberies that took place around the Detroit area in 2011.[11] Initially, police officers arrested four men other than Carpenter for the robberies, and one confessed to robbing nine stores in Michigan and Ohio.[12] The same suspect revealed there were fifteen accomplices in the heists and gave up some of their cell phone numbers to the FBI.[13] Timothy Carpenter's phone number was among the phone numbers on the list that the FBI received.

Relying on the SCA, the prosecutors applied for court orders and obtained Carpenter's historical cell site information from the four-month time frame when the robberies occurred.[14] Federal magistrate judges issued two orders to Carpenter's cellular service providers, MetroPCS and Sprint: the first order sought 152 days of cell-site records from MetroPCS, and the

6. Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 431 (2007).

7. *Id.*

8. Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1747–48 (2009).

9. NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, CELL PHONE LOCATION TRACKING, https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/LQ8K-2KF3] [hereinafter NACDL].

10. *Carpenter*, 138 S. Ct. at 2221.

11. *Id.* at 2212.

12. *Id.*

13. *Id.*

14. *Id.*

second order sought seven days of cell-site records from Sprint.[15] The orders produced 127 days of records and two days of records from MetroPCS and Sprint, respectively.[16]

Based on the cell-site data provided by wireless carriers, Carpenter was charged with multiple counts of both robbery and "carrying a firearm during a federal crime of violence."[17] Carpenter's chief argument relied on the Fourth Amendment. Carpenter argued his Fourth Amendment rights were violated when the Government seized CSLI from his wireless carriers absent the traditional probable cause requirement, and he moved to suppress the records before trial.[18] The district court denied the motion, and at trial an FBI agent's expert testimony about CSLI placed Carpenter's phone near four of the robberies at the time the robberies occurred.[19] Consequently, Carpenter was convicted on all counts except for one of the firearm counts, and he was sentenced to over 100 years in prison.[20]

At the appellate level, the Sixth Circuit affirmed the lower court's decision, holding Carpenter had no reasonable expectation of privacy in the CSLI because he voluntarily shared the data with each of his cellular service providers.[21] Thus, Carpenter could not claim that his Fourth Amendment rights protected the disclosure of those resulting business records.[22] The Supreme Court granted certiorari.

B. Reasoning

In *Carpenter*, the Supreme Court delivered two significant holdings: (1) accessing at least seven days of CSLI constitutes a search under the purview of the Fourth Amendment given the legitimate expectation of privacy in physical movements captured by CSLI; and (2) to access those CSLI records, a warrant supported by probable cause is required.

The first of the two primary holdings is important for understanding the type of information that is under the Fourth Amendment's purview and to what extent the Court is willing to extend Fourth Amendment doctrine in an increasingly technological world. Arguably, the second holding concerning warrants and subpoenas is of greater significance as it potentially

15. *Id.*
16. *Id.*
17. *Id.*; *see also* 18 U.S.C. § 924(c) (2006).
18. *Carpenter*, 138 S. Ct. at 2212.
19. *Id.* at 2212–13.
20. *Id.* at 2213.
21. *Id.*
22. *Id.*

calls a subpoena's utility into question. Section III will address the Fourth Amendment's relation to warrants and subpoenas—and the difference between the two.

Chief Justice Roberts wrote the opinion, and there was a clear majority with the decision being 5-4. The four liberal-leaning Justices—Justice Ginsburg, Breyer, Kagan, and Sotomayor—joined the Chief Justice. In turn, Justice Kennedy, Thomas, Alito, and Gorsuch each wrote separate dissenting opinions. In particular, Justice Alito's dissent emphasized the negative implications for subpoena practice.

The Government's access of Carpenter's cell-site records was a search under the Fourth Amendment.

Writing for the majority, Chief Justice Roberts was tasked with explaining how the Fourth Amendment works in light of a "new phenomenon"; that is, the new capability to obtain all of an individual's past movements by accessing his or her cell phone records.[23] The first step, as is true for most Fourth Amendment questions, was to decide whether obtaining Carpenter's cell-site data from his wireless carriers would be considered a search under Fourth Amendment doctrine.

In pertinent part, the Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[24] Its main purpose is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[25] Repudiating the old Fourth Amendment doctrine traditionally linked with common-law trespass, the Court reestablished it is "people, not places," that the Fourth Amendment protects.[26] For an official action to be considered a Fourth Amendment search, it must have violated an individual's subjective expectation of privacy "that society is prepared to recognize as reasonable."[27] In turn, access to that private information requires a warrant supported by probable cause.[28]

The Court is intent on protecting individual privacy against arbitrary and pervasive police power by acknowledging that Fourth Amendment boundaries will be stretched as technology becomes more advanced.[29] For example, the Court has applied the Fourth Amendment flexibly in some

23. *Id.* at 2216.
24. U.S. CONST. amend. IV.
25. New Jersey v. T.L.O., 469 U.S. 325, 335 (1985).
26. *Carpenter*, 138 S. Ct. at 2213; Katz v. United States, 389 U.S. 347, 351 (1967).
27. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
28. *Carpenter*, 138 S. Ct. at 2213.
29. *Id.* at 2214; McLaughlin, *supra* note 6, at 429–30.

cases to make sure that an individual's privacy was not left to "the mercy of advancing technology."[30]

Carpenter marks the first instance where the Court considered the Government's warrantless access to an individual's cell-site location data through his wireless carrier. The reasoning employed in existing precedents did not easily agree with the facts—specifically, the cell-site data—in this case.[31] Largely, the Court relied on *United States v. Jones*, where the Government tracked an individual's movements for 28 days after placing a GPS tracking device on his vehicle.[32] While *Jones* was decided based on trespass principles, the concurring opinions indicated that long-term GPS tracking in investigations often infringe on expectations of privacy and may require a warrant.[33]

Similar to the GPS tracking in *Jones*, CSLI is "detailed, encyclopedic, and effortlessly compiled."[34] According to the Government, however, the third-party doctrine should have controlled the outcome of *Carpenter*.[35] Based on *United States v. Miller*[36] and *Smith v. Maryland*,[37] the Government asserted it was free to obtain Carpenter's cell-site records without infringing his Fourth Amendment rights because he voluntarily turned that data over to a third party.[38] Still, because the data conveyed to third parties in this case gave a "detailed and comprehensive record of [Carpenter's] movements," the fact that the data rested with a third party was not enough to overcome Carpenter's Fourth Amendment concerns.[39]

In the majority's view, the privacy concerns surrounding CSLI are more troubling than those encountered when the Government monitors a vehicle with a tracking device.[40] An individual's reasonable expectation of privacy extends to "the whole of [his] physical movements" and, consider-

30. *See* Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (holding that federal agents conducted a Fourth Amendment search when they used a thermal imaging device scan an individual's home).

31. *Carpenter*, 138 S. Ct. at 2214.

32. 565 U.S. 400, 404–05 (2012).

33. *Id.* at 430 (Alito, J., concurring in judgment); *Id.* at 415 (Sotomayor, J., concurring).

34. *Carpenter*, 138 S. Ct. at 2216.

35. *Id.* at 2219.

36. 425 U.S. 435, 443 (1976) (holding that a bank patron had no expectation of privacy in the financial records held by his bank).

37. 442 U.S. 735, 745 (1979) (holding that an individual had no expectation of privacy in records of dialed telephone numbers kept with a telephone company).

38. *Carpenter*, 138 S. Ct. at 2219.

39. *Id.* at 2216–17, 2220. For a discussion about the status of the third-party doctrine, *see* Orin S. Kerr, *First Thoughts on Carpenter v. United States*, VOLOKH CONSPIRACY (Jun. 22, 2018, 12:20 PM), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta [https://perma.cc/M5HG-K59T].

40. *Carpenter*, 138 S. Ct. at 2218.

ing individuals are rarely without their cell phones, government access to cell phone location records allows almost perfect surveillance of a cell phone user's movements.[41] Accordingly, the Government accessing Carpenter's cell-site records—even while they were stored with a third party—constituted a Fourth Amendment search.[42]

The Government must have obtained a warrant supported by probable cause before accessing Carpenter's cell-site records.

After finding the Government's access to Carpenter's cell-site records constituted a Fourth Amendment search, the Court questioned what standard the government must satisfy in order to lawfully acquire those records.[43] When law enforcement officials conduct a search to discover evidence of a crime without a warrant, the search is typically deemed unreasonable unless it qualifies as an exception to the warrant requirement.[44]

Here, the Government compelled Carpenter's wireless carriers to disclose his cell-site records by obtaining a court order under Section 2703(d) of the Stored Communications Act.[45] Court orders are only issued under Section 2703(d) if the Government or governmental entity shows "reasonable grounds" to believe that the records sought are "relevant and material to an ongoing criminal investigation."[46] Compared to the standard required for a warrant—probable cause—the Section 2703(d) standard is clearly less demanding.[47] Accordingly, the Government's use of court-approved compulsory process under the SCA was an invalid method for accessing an individual's CSLI—a warrant was still required.[48]

Chief Justice Roberts then turned to the contrary arguments in Justice Alito's dissenting opinion. For Justice Alito, the compulsory production of documents is merely a "constructive search" that is far less intrusive on an individual's privacy than an "actual search," and the warrant requirement should not apply in such instances.[49] In theory, a subpoenaed individual conducts the search for the relevant documents himself and avoids any inadvertent invasions of privacy that might accompany an actual search conducted by a governmental official.[50] Thus, a court order to produce

41. *Id.* at 2219. The majority notes that the technology considered in this case is "rapidly approaching GPS-level precision." *Id.*

42. *Id.* at 2220.

43. *Id.* at 2221.

44. *Id.*

45. *Id.*

46. 18 U.S.C. § 2703(d) (2018); *Carpenter*, 138 S. Ct. at 2221.

47. *Carpenter*, 138 S. Ct. at 2221.

48. *Id.*

49. *Id.* at 2255 (Alito, J., dissenting).

50. *Id.* at 2252 (Alito, J., dissenting).

documents should not be treated like an actual search that requires probable cause.[51]

But the majority again stressed that CSLI is wrought with Fourth Amendment privacy concerns that far outweigh those that accompany "corporate tax or payroll ledgers" mentioned in the examples Justice Alito cites.[52] If Fourth Amendment protection did not apply to the subpoena process as Justice Alito suggests, the majority asserts the warrant requirement would no longer be able to protect any type of record, and the government could subpoena any document based only on "official curiosity."[53] The majority was not willing to adopt that categorical limitation on the Fourth Amendment.

Regardless of the majority's reassurances, Justice Alito fears that imposing the requirements governing actual searches and seizures on a court order to produce documents is "revolutionary" and will hinder investigations of significant offenses.[54]

II. THE SCA AND TWO COMPETING STANDARDS TO PRODUCE DOCUMENTS

In criminal procedure, there are traditionally two kinds of legal process available when the Government wants to gain access to some sort of incriminating evidence—namely, the search warrant and subpoena process.[55] The two paths are distinguishable in that their execution is regulated by two different legal regimes.[56] For a search warrant, the Fourth Amendment limits and imposes a higher standard on investigators.[57] Issuing a grand jury subpoena, on the other hand, may be done without abiding by the stringent requirements for a search warrant. The Fourth Amendment still applies in the subpoena context, but its presence is not very significant for reasons discussed below.

If search warrants and grand jury subpoenas are at opposite ends of the spectrum in terms of the legal standard involved to obtain evidence, then the process laid out in Section 2703(d) of the Stored Communications Act is somewhere in between. The "2703(d)" order could be described as

51. *Id.* at 2221.

52. *Id.* at 2222.

53. *Id.* (quoting United States v. Morton Salt Co., 338 U.S. 632, 652 (1950)).

54. *Id.* at 2247 (Alito, J., dissenting).

55. Orin S. Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, VOLOKH CONSPIRACY (Jun. 26, 2018, 5:36 PM), http://reason.com/volokh/2018/06/26/does-carpenter-revolutionize-the-law-of [https://perma.cc/QC4D-DBCW].

56. *Id.*

57. *Id.*

"a mix between a subpoena and a search warrant."[58] Nonetheless, the Court in *Carpenter* held the Congress-prescribed standard for compelling production of records featured in the SCA could not pass muster Fourth Amendment scrutiny—at least in the CSLI context—and a warrant is still required to access those records.[59]

The *Carpenter* holding raises several concerns about subpoena practice: (1) Whether and how the holding affects grand jury or administrative subpoenas, where there is seemingly a lower standard to meet; and (2) Whether warrants now subsume the role of subpoenas from grand juries and administrative agencies, alike. To begin answering some of these questions, understanding the legal processes available for obtaining documents and their relative standards is imperative.

A. The Warrant Requirement

In criminal investigations, the most familiar legal mechanism used to obtain evidence is the search warrant.[60] A valid search warrant allows investigators to physically intrude into a private area in order to obtain information; however, the Fourth Amendment offers individual protections—applied to both criminal and civil investigations—that generally place limits on investigators.[61] Under the Fourth Amendment, people are afforded the right "to be secure in their persons, houses, papers, and effects," and to be protected "against unreasonable searches and seizures."[62] The Amendment also requires probable cause to accompany each warrant a magistrate or judge issues.[63]

At the forefront, the Fourth Amendment was adopted "to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[64] Without the clear authority of law, government officials have no right to interfere with an individual's personal security, which is "sacred."[65] And "the protection against warrantless searches and seizures" works to ensure that a neutral magistrate's judgment acts as a buffer

58. 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 (2004).

59. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

60. Kerr, *supra* note 55.

61. *Id.*

62. U.S. CONST. amend. IV.

63. *Id.*

64. *T.L.O.*, *supra* note 25, at 335.

65. Terry v. Ohio, 392 U.S. 1, 9 (1968).

between individuals and the unbridled power of a government "official caught up in the heat of an investigation."[66]

Accordingly, warrantless searches are per se unreasonable.[67] Even though the Fourth Amendment does not necessarily require a warrant or probable cause to support a search, the Supreme Court has held a warrant is presumably required for searches and seizures unless "a specific exception to the warrant requirement" applies.[68]

While most warrantless searches are done upon consent, other exceptions to the warrant requirement exist only in rare circumstances. The constitutionality of a warrantless Fourth Amendment search turns on a question of reasonableness, determined by "balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[69] Where special law enforcement needs, low expectations of privacy, and minimal intrusions exist, a warrantless search is more likely to be considered reasonable, and, thus, constitutional.[70]

1. Probable Cause

Aside from special circumstances, investigators generally need a warrant supported by probable cause to conduct an official search protected by the Fourth Amendment. After all, the warrant requirement is partially based on the idea that any search or seizure is inherently wrong and should not be executed without first determining whether the action is truly necessary.[71] And if a search must take place, the scope of the search should be limited.[72]

A search warrant requires a different factual showing than an arrest warrant, given that the two protect different interests listed in the Fourth Amendment.[73] While an arrest warrant addresses an individual's right against unreasonable seizures, search warrants protect an individual's "rea-

66. 79 C.J.S. *Searches* § 16 (2018).

67. *See, e.g.*, City of Los Angeles, Calif. v. Patel, 135 S. Ct. 2443, 2452 (2015) (concluding a municipal code requiring hotel operators to provide police with information about guests was unconstitutional); Arizona v. Gant, 556 U.S. 332, 338 (2009); Katz v. United States, 389 U.S. 347, 357 (1967). *See* 79 C.J.S. *Searches* § 15 (2018).

68. *See Investigations and Police Practices*, 47 GEO. L.J. ANN. REV. CRIM. PROC. 3, 4 n.4 (2018) [hereinafter *Investigations*]; Riley v. California, 573 U.S. 373, 382 (2014) (A warrantless search is unreasonable unless "it falls within a specific exception to the warrant requirement").

69. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995) (quoting Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, 617 (1989)) (concluding that random urinalysis tests of student athletes were reasonable under the Fourth Amendment considering the state's legitimate interests and the intrusiveness of the tests).

70. 79 C.J.S. *Searches* § 15 (2018).

71. *See* Searches, *supra* note 66.

72. *Id.*

73. *Investigations*, *supra* note 68, at 25.

sonable expectation of privacy"[74] and possessions against government intrusion. These protections hold especially true for individuals in their own home; although, the Supreme Court has articulated that "the Fourth Amendment protects people, not places."[75]

A magistrate may only issue a search warrant after investigators show "probable cause to believe that the legitimate object of a search is located in a particular place."[76] "[P]robable cause is a flexible, common-sense standard" that depends on the totality of the circumstances in each case.[77] Still, the factual showing required for probable cause is significant—a reasonable and unbiased mind must be persuaded to believe a crime has actually occurred as opposed to causing mere suspicion or speculation of a crime.[78]

Probable cause does not require certainty on the belief that the sought evidence will establish a prima facie element of a crime.[79] Instead, what is relevant is the probability that a crime has occurred and the probability that criminal evidence exists and will be found.[80] In assessing these probabilities, magistrates consult all the facts and circumstances within the warrant application using a "practical, common-sense" approach.[81]

2. The Particularity Requirement

To avoid "wide-ranging exploratory searches," a search warrant must describe with particularity the places that will be searched and the people or objects that will be seized under the Fourth Amendment.[82] The requirement ensures searches are narrowly tailored to the justification making them necessary at the outset and prevents, among other things, warrants from being issued without an adequate factual basis or probable cause.[83]

Like probable cause, the totality of circumstances in each case determines whether a search warrant describes a place with sufficient particularity—the description ought to be as precise as possible given the circumstances.[84] The particularity question also considers whether the war-

74. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
75. *Id.* at 351.
76. Steagald v. United States, 451 U.S. 204, 213 (1981).
77. 79 C.J.S. *Searches* § 67 (2018).
78. *Id.*
79. *Id.*
80. *Id.*
81. Illinois v. Gates, 462 U.S. 213, 238 (1983); *Investigations*, *supra* note 68, at 28.
82. Maryland v. Garrison, 480 U.S. 79, 84 (1987); U.S. CONST. amend. IV.
83. 79 C.J.S. Searches § 235 (2018).
84. 79 C.J.S. Searches § 236 (2018).

rant provides adequate protection for an individual's privacy and personal rights, and whether the warrant puts the party searched on proper notice.[85]

The description within the warrant should be precise enough so as to leave the executing officer without the opportunity to exercise any of his or her own discretion during the search.[86] But when a warrant is overbroad or otherwise mistaken, an executing officer may use his or her personal knowledge to narrow down the intended search area.[87]

3. The Grand Jury Subpoena

Indeed, warrants are often used during criminal investigations. But the warrant is not the only legal process available to obtain information—the subpoena is the primary mechanism the Government uses routinely to collect records and other documents.[88] Grand juries issue thousands of these each year.[89]

As distinguished from a search warrant, which allows government officials to physically intrude on private property in search of incriminating evidence, a subpoena duces tecum directs a recipient to gather evidence his or herself and bring the evidence to a grand jury at a later date.[90] A third-party witness may also be summoned to testify in front of a grand jury with a subpoena ad testificandum.[91]

By using a subpoena, the Government may obtain access to various kinds of "papers" with a far lesser showing than probable cause. In that main respect, the law regarding grand jury subpoenas is very different from the law governing warrants—which also explains why subpoenas are preferable to search warrants when it comes to requesting routine documents.

A subpoena, unlike a search warrant issued ex parte, may be challenged by the recipient before compliance.[92] Under the Fourth Amendment, the only refuge available to a recipient is arguing that the subpoena is overbroad, irrelevant, or too burdensome to comply with.[93] Courts show extreme deference to the grand jury and, consequently, these objections rarely

85. *Id.*
86. Steele v. United States, 267 U.S. 498, 503 (1925).
87. *Investigations*, *supra* note 68, at 34.
88. Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 805 (2005).
89. *Id.*
90. Kerr, *supra* note 55.
91. 98 C.J.S. *Witnesses* § 21 (2018).
92. Slobogin, *supra* note 88, at 806, 810.
93. *Id.* at 806; United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108 (9th Cir. 2012); In re Grand Jury Subpoena, 920 F.2d 235, 243–244 (4th Cir. 1990).

prevail.[94] For example, there would have to be "no reasonable possibility" that the information the Government is seeking relates to the subject matter of the grand jury's investigation in order for a subpoena to be struck down as irrelevant.[95]

Still, a recipient may challenge a subpoena using another means, namely, his Fifth Amendment privilege against self-incrimination. In a unique circumstance when responding to a subpoena duces tecum, an individual may be able to assert Fifth Amendment privilege if the act of producing the documents requested conveys additional information that may be incriminating.[96] Usually, the Fifth Amendment privilege is unavailable.[97]

Consequently, grand jury subpoenas duces tecum are easily enforced.[98] They are controlled and issued in the name of the grand jury; but, in reality, the prosecutors who manage the grand jury are behind each subpoena—prosecutors ask for, draft, serve, and defend each subpoena.[99] Nonetheless, the Supreme Court has traditionally held grand jury subpoenas to a low standard, indicating that a subpoena seeking to satisfy "nothing more than official curiosity" is constitutional.[100] The Government may use a subpoena to acquire documents so long as "the documents sought are relevant to the [investigation]" and the document request is "adequate, but not excessive," for those same purposes.[101]

Before *Carpenter*, subpoenas aimed at third-party recordholders seemed to be unrestricted. The phenomenon was especially concerning given that modern society often requires personal information be kept with some third party—and third parties are unable to plausibly assert the Fifth Amendment privilege over someone else's information.[102] In the same context, the third-party doctrine curtailed any Fourth Amendment claims

94. Slobogin, *supra* note 88, at 806.

95. United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (rejecting a company's challenge to grand jury subpoenas for corporate records because it did not establish there was no reasonable possibility the information produced would be relevant to the grand jury's investigation).

96. Fisher v. United States, 425 U.S. 391, 411 (1976) (noting that a party conceding that it possesses the requested papers is a foregone conclusion and does not add any useful incriminating information to the investigation).

97. Slobogin, *supra* note 88, at 806.

98. *Id.*

99. Kerr, *supra* note 55.

100. United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) (concluding agencies have a right to request information from corporations even if for no other reason than "official curiosity").

101. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946) (upholding the production of a newspaper publishing corporation's books and records as request was made pursuant to statute and was reasonably relevant).

102. Slobogin, *supra* note 88, at 808.

over information voluntarily shared with a third party.[103] Now, *Carpenter* at least signifies that conveying information to a third party is but a factor in determining whether an individual has a reasonable expectation of privacy in such information—the conveyance is not dispositive.

B. The Stored Communications Act

Enacted as Title II of the Electronic Communications Privacy Act of 1986, the SCA regulates both the voluntary and compelled disclosure of stored internet communications records retained by internet service providers.[104] Largely, Congress enacted the SCA to bridge the gap between legitimate Fourth Amendment concerns and the internet's general structure.[105] The Fourth Amendment, while generally ensuring strong protections for individuals in their homes, might not offer those same protections to individuals operating online.[106] For example, the Government must obtain a search warrant supported by probable cause to search someone's home for a letter in a desk drawer but only needs a subpoena to access that same letter remotely stored in a Google web account under the third-party doctrine.[107] The letter clearly has much less protection in the latter scenario. Consequently, the SCA works to provide network account holders with various statutory rights making access to their stored account information more secure.[108]

Under the SCA, the government typically seeks two types of information: (1) contents of wire or electronic communications in electronic storage and remote computing services[109]; and (2) "records concerning electronic communication service[s] or remote computing service[s]," which notably do not contain the contents of communications.[110] Cell-site location information falls under the latter category; the information does not qualify as the "contents of communications."[111] Thus, Section 2703(c), which addresses the disclosure of "a record or other information pertaining

103. *See* United States v. Miller, 425 U.S. 435, 443 (1976). Craig Ettinger, *Does the History Behind the Adoption of the Fourth Amendment Demand Abolishing the Third-Party Doctrine?*, 29 GEO. MASON U. CIV. RTS. L.J. 1, 19–23 (2018), for a general discussion about the third-party doctrine and its creation.

104. *See* 18 U.S.C. §§ 2701–2711 (2018).

105. Kerr, *supra* note 58, at 1209 (explaining the structure of the Stored Communications Act and suggesting Congress amend the statute to better protect individuals' stored internet communications).

106. *Id.* at 1209–10.

107. *Id.* at 1209, 1212.

108. *Id.* at 1212.

109. 18 U.S.C. § 2703(a)–(b) (2018).

110. § 2703(c).

111. Chamberlain, *supra* note 8, at 1756.

to a subscriber to or customer of [a provider of electronic communication or remote computing] service," applies when the government seeks access to CSLI.[112]

Before *Carpenter*, the SCA ostensibly provided the government with three avenues it could take to compel the disclosure of CSLI records.[113] First, pursuant to the Federal Rules of Criminal Procedure, a governmental entity can obtain a warrant.[114] Instead of using the process required for a warrant, investigators could either obtain "the consent of the subscriber or customer to such disclosure"[115] or compel disclosure with a court order under Section 2703(d).[116] In pertinent part, Section 2703(d) states:

> A court order for disclosure . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[117]

Notably, the Government in *Carpenter* abided by the requirements laid out in Section 2703(d) of the SCA in order to access Carpenter's cell-site location information through a court order.[118] A magistrate found the Government had offered "specific and articulable facts showing that there are reasonable grounds to believe that . . . records or other information sought, are relevant and material to an ongoing criminal investigation" and issued two court orders.[119] Investigators serve court orders under Section 2703(d) just like they would an ordinary subpoena—by bringing the order to the service provider who then provides investigators with the information sought.[120]

Holding that access to Carpenter's CSLI nonetheless required a warrant seemingly does not undermine two of the relevant processes (obtaining a warrant or prior consent) available to the government listed in Section 2703(c); however, when seeking sensitive information akin to CSLI and the probable cause requirements are satisfied, the Government would presumably elect to issue a warrant, displacing the subpoena process.[121]

112. *See* § 2703(c); Chamberlain, *supra* note 8, at 1756.
113. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018); Kerr, *supra* note 58, at 1218–19.
114. *See* § 2703(c).
115. *Id.*
116. *Id.*
117. § 2703(d).
118. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
119. *See* § 2703(d); *Carpenter*, 138 S. Ct. at 2212.
120. *See* Kerr, *supra* note 58, at 1219.
121. Marty Lederman, Carpenter's *Curiosities (and its Potential to Unsettle Longstanding Fourth Amendment Doctrines)*, BALKINIZATION (June 26, 2018),

Indeed, the Court's holding is just as significant of a triumph for privacy rights as it is a departure from traditional subpoena practice and the third-party doctrine.

III. A FOURTH STANDARD: ADMINISTRATIVE SUBPOENAS OR SUMMONS

Created through statute, many federal administrative agencies are charged with implementing regulatory or fiscal policies.[122] In order to fulfill those duties, agencies need sufficient investigatory power to access information, which is largely derived from an agency's power to subpoena records and testimony.[123] Congress authorizes this power through a statute, namely, the Administrative Procedure Act ("APA") that grants agencies subpoena power if another statute authorizes issuance.[124] Thus, each agency has its own enabling statute granting it the power to issue administrative subpoenas.[125]

Today, administrative agencies have broad power to issue subpoenas without prior approval from a grand jury or court.[126] Individuals and entities subject to agency regulation often have an incentive to cooperate with the agency's subpoena or voluntarily produce documents or testimony.[127] But administrative subpoenas are not self-enforcing, and agencies need to bring the subpoena to a federal judge in order to compel document or testimony production from those who choose not to comply.[128] Further failure to comply with a court order may result in the target being held in contempt.[129]

https://balkin.blogspot.com/2018/06/carpenter-s-curiosities-and-its.html [https://perma.cc/EE8N-SLEZ] (arguing that the *Carpenter* holding has "groundbreaking" implications for national subpoena practice).

122. *See* U.S. DEP'T OF JUSTICE, OFFICE OF LEGAL POLICY, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES (2002) [hereinafter DOJ Report], https://www.justice.gov/archive/olp/rpt_to_congress.htm#b19 [https://perma.cc/75YL-23DN].

123. *See* Graham Hughes, *Administrative Subpoenas and the Grand Jury: Converging Streams of Criminal and Civil Compulsory Process*, 47 VAND. L. REV. 573, 579, 584 (1994).

124. *See* 5 U.S.C. § 555(d) (1966); COMPULSORY PROCESS, 1 Admin. L. & Prac. § 3:12 (Charles H. Koch, Jr. & Richard Murphy eds., 3d ed. 2019).

125. *See* DOJ REPORT, *supra* note 122.

126. *Id.*

127. *See* Abraham Tabaie, *Protecting Privacy Expectations and Personal Documents in Sec Investigations*, 81 S. CAL. L. REV. 781, 797 (2008) (arguing that an entity being viewed as "cooperative" with the SEC may be important in resolving the Commission's inquiry).

128. *See, e.g.*, Sec. Exch. Cmm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741 (1984) (SEC subpoena is not self-enforcing); Wearly v. Fed. Trade Comm'n, 616 F.2d 662, 665 (3d Cir.1980).

129. *See* 5 U.S.C. § 555(d) (1966); SUBPOENAS, ADMINISTRATIVE LAW PRACTICE AND PROCEDURE § 2:4 (Lee Modjeska ed., 2019).

Courts have not always respected administrative subpoena power.[130] But with the introduction of New Deal initiative and in the aftermath of economic crisis, the administrative state grew, and courts began affording administrative subpoena enforcement more deference.[131] While not without its limits, the highly deferential standard has now governed administrative subpoena enforcement for over seventy years.[132]

Indeed, the expansion of administrative investigatory power is derived from the principle that excess judicial interference would hinder agencies' ability to execute their statutory responsibilities.[133] As such, administrative subpoenas are subject to a "reasonableness" standard, which requires a far lesser showing than what is required under the "probable cause" standard associated with issuing a valid search warrant.[134] Courts today frequently cite *United States v. Powell*, where the Supreme Court concluded the Internal Revenue Service did not need to meet the probable cause standard to enforce its administrative summons requesting corporate tax records.[135] Instead, the Court articulated a four-factor evaluation for deciding whether a summons could be enforced, requiring that (1) the investigation is conducted for a legitimate reason; (2) the inquiry is relevant to the investigation's purpose; (3) the agency does not already have the information sought; and (4) the agency has followed the proper administrative steps in issuing the subpoena.[136] While decided in the context of an IRS enforcement action, *Powell* is generally applicable to all administrative agencies.[137]

Prior to *Powell*, administrative subpoenas seeking evidence "not plainly incompetent or irrelevant to any lawful purpose of the [requesting officer] in the discharge" of his or her statutory responsibilities were

130. *See* Fed. Trade Comm'n v. Am. Tobacco Co., 264 U.S. 298, 305–06 (1924) (prohibiting the Federal Trade Commission from acquiring a corporation's letters and wires through a subpoena).

131. *See* Tabaie, *supra* note 127, at 789.

132. *See* Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943) (enforcing an administrative subpoena requesting a corporation's payroll records because the records sought were not "plainly incompetent or irrelevant to any lawful purpose").

133. *See* Hughes, *supra* note 123, at 584 (1994) (asserting the arrangement between the government and those engaged in licensed commercial activities would be "unworkable" without compulsory process).

134. *See, e.g.*, United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) (government requests for corporate books and records are enforceable without a warrant as long as "the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant").

135. *See* 379 U.S. 48, 57 (1964).

136. *Id.* at 57–58.

137. *See* Sec. Exch. Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741–42 (1984) (applying *Powell* standards in litigation about enforcing an SEC subpoena).

enforceable.[138] The Court reinforced this idea in *United States v. Morton Salt Co*., indicating that an administrative subpoena is appropriate even if the demand amounts to a mere "fishing expedition" designed only to confirm compliance with regulatory requirements.[139] So long as the agency has the authority to inquire, the demand for information is not too indefinite, and the sought after information is "reasonably relevant," enforcing an administrative subpoena is appropriate.[140] Courts even defer to the agency's determination in what information is "reasonably relevant" to an investigation barring a scenario where the court deems the agency is "obviously wrong."[141] Some of this deference results from agencies having developed considerable expertise in technical areas such as taxation, securities, health and safety, or airplane design and safety. Consequently, administrative agencies enjoy significant leniency while seeking information and do not necessarily need to connect the information sought to any actual theory of violation.[142]

Administrative subpoena enforcement and its doctrine has mirrored that of grand jury subpoenas over the years, and some scholars argue the two forms of compulsory process are completely assimilated.[143] Notably, enforcing either type of subpoena would be subject to similar standards and scrutiny.[144] But the justifications behind the grand jury as an investigative body arguably contain a crucial component absent from administrative investigations—that a grand jury functions to investigate and prosecute crime while protecting citizens from "unfounded criminal charges." In theory, grand juries are independent, democratic institutions composed of cooperating citizens and peers, which affords them special legitimacy in American jurisprudence.[145] Neither of these justifications are applicable to administrative agencies, even though agencies take advantage of the same broad authority to gather information.[146] However, agencies are part of the

138. Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943).

139. *See* 338 U.S. at 642–43 (attributing the power to "investigate merely on suspicion that the law is being violated" to administrative agencies while analogizing agencies to grand juries); *Powell*, 379 U.S. at 57.

140. *Morton Salt Co*., 338 U.S. at 652.

141. *See* Fed. Trade Comm'n v. Texaco, Inc., 555 F.2d 862, 877 (D.C. Cir. 1977) (concluding that the FTC's request for a natural gas producer's bid files was "reasonably relevant" to its investigation, and the FTC's theory about the bid files was not "obviously wrong").

142. *See id.* at 877.

143. *See generally* Hughes, *supra* note 123 (discussing the judicial approach to civil investigative demands being based on grand jury principles).

144. *See id.* at 594–95.

145. *See id.* at 581–82; *but see* Kerr, *supra* note 55 (noting the prosecutors actually have control over the grand jury).

146. *See* Hughes, *supra* note 123, at 589.

executive branch and are subject to Congress' oversight abilities; if they become overly aggressive, the President could be held accountable.

In *Carpenter*, the Government analogized a 2703(d) order to a grand jury subpoena, arguing that the order is an acceptable form of compulsory process under the Fourth Amendment for the same reasons as grand jury and administrative subpoenas. Rejecting the Government's argument, the Court concluded the Fourth Amendment requires a judicially issued warrant to compel disclosure of CSLI records, even if it had been a grand jury or administrative agency wishing to issue a subpoena for the same records.

A. Government's Grand Jury Argument in Carpenter

Referencing the standard articulated in the seminal case, *Oklahoma Press Publishing Co. v. Walling* ("*Oklahoma Press*"), the Government argued its 2703(d) order is similar to a grand jury subpoena duces tecum and the Fourth Amendment allows it to subpoena documents as long as Congress authorized the investigation "for a purpose Congress can order," the sought-after documents are relevant to the inquiry, and the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry."[147] The Government argued that, on balance, the level of intrusiveness a subpoena imposes on an individual does not outweigh the significant governmental interest acquiring information during the early stage of an investigation serves.[148]

On the privacy side, compulsory process is justified considering the subpoena target is requested to bring forth documents as opposed to the government finding the information itself. Further, intrusion is limited as a subpoena recipient may object before producing documents to the government.[149] Conversely, requiring a warrant supported by probable cause during the early stages of an investigation would significantly hinder investigations in the public interest and render investigative duties nearly impossible.[150] The Government asserted that its ability to investigate would suffer if it were required to establish probable cause to issue a subpoena when "the very purpose of requesting the information is to ascertain whether probable cause exists."[151]

147. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946).

148. Brief for the United States at 45–46, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16–402), 2017 WL 4311113.

149. *See Okla. Press*, 327 U.S. at 195.

150. *See id.* at 213.

151. United States v. R. Enters., Inc., 498 U.S. 292, 297 (1991).

Alluding to grand jury and administrative subpoenas, the Government emphasized that 2703(d) orders pursuant to the Stored Communications Act share similar features to other forms of compulsory process validated by courts without a warrant in that recipients bring forth the requested records and can object to the production in court, and the government often relies on 2703(d) orders in preliminary investigations.[152]

Certainly, the standard prescribed in the SCA for compelling CSLI disclosure is more demanding than the standard imposed on a grand jury (or an administrative agency) to issue a valid subpoena.[153] Congress decided on this standard after holding numerous hearings and debates. By ruling out the SCA standard as insufficient, the Court is supplanting Congress's will as the voice of the People.

As stated, a 2703(d) order requires the Government to establish "reasonable and articulable facts" about the requested information being "relevant and material to an ongoing criminal investigation."[154] And compelling disclosure pursuant a 2703(d) order requires judicial approval. By comparison, a subpoena duces tecum must be merely relevant to the Government's investigation, and the documents requested need to be "adequate, but not excessive" for the same purposes.[155] Issuing a subpoena typically does not require judicial involvement, but enforcing a subpoena after a recipient chooses not to comply requires a court order.

Nonetheless, both grand juries and administrative agencies are afforded great deference in subpoena enforcement. Intuitively, given that Congress's 2703(d) standard clearly satisfies the low subpoena requirements and offers more protection to a recipient, it follows that the 2703(d) order would be sufficient under the Fourth Amendment. But the subpoena analogy did not serve the Government, as the Court concluded the warrant requirement would still have been required even if a grand jury or administrative agency had issued a subpoena for the CSLI records.

Admittedly, the scope of the Court's holding beyond a 2703(d) order seeking location information is unclear. The question is open as to whether courts will apply *Carpenter*'s broad reasoning when evaluating government access to sensitive or personal information unrelated with location, which could be problematic for an individual or company considering how to respond to a subpoena.

152. Brief for the United States at 46, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16–402), 2017 WL 4311113.

153. *See id.*

154. 18 U.S.C. § 2703(d).

155. *Okla. Press*, 327 U.S. at 209.

Justice Alito uses the SEC as an example of a federal agency with power to request documents through an administrative subpoena. Like other agencies, the SEC has expansive investigative power in the name of "investor protection" to obtain both business-related information and documents containing personal information such as medical, financial, and email data.[156] According to Alito, any order compelling the production of documents containing sensitive information will now require a showing of probable cause.[157] If that is the case, agencies that routinely obtain a wide range of information from individuals or companies—like the SEC—may lose some discretion in deciding which investigative leads to pursue and which data to obtain a warrant for.[158]

B. The Securities and Exchange Commission

1. History and Creation

In response to the worst economic crisis in American history, Franklin D. Roosevelt enacted a myriad of legislative programs dubbed the "New Deal," which aimed to centralize federal government control over the economy. Among the legislative programs enacted within FDR's first hundred days in office was the Securities Act of 1933 (the "'33 Act")—the first act of a collection that would eventually become known as the federal securities laws. The Great Depression and Wall Street crash of 1929 provided the fuel necessary for Congress to create legislation governing the securities industry, an area in which states' "blue sky" laws previously had autonomy. Today, there are eight primary acts governing the capital markets industry: the Securities Act of 1933, the Securities Exchange Act of 1934, the Trust Indenture Act of 1939, the Investment Company Act of 1940, the Investment Advisers Act of 1940, the Sarbanes-Oxley Act of 2002, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, and the Jumpstart Our Business Startups Act of 2012.[159]

156. *See* Slobogin, *supra* note 88, at 806–07; Sec. Exch. Comm'n v. Ralston Purina Co., 346 U.S. 119, 124 (1953) (the intent of the Securities Act is "to protect investors by promoting full disclosure of information thought necessary to informed investment decisions").

157. Carpenter v. United States, 138 S. Ct. 2206, 2260–61 (2018) (Alito, J., dissenting).

158. *See* Paul Ohm, *The Broad Reach of Carpenter v. United States*, JUST SECURITY (June 27, 2018), https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states/. [https://perma.cc/3A6P-KSCH]

159. *The Laws that Govern the Securities Industry*, U.S. SEC. AND EXCH. COMM'N, https://www.sec.gov/answers/about-lawsshtml.html [https://perma.cc/U9H7-6JZU] (last modified Oct. 1, 2013) [hereinafter THE LAWS THAT GOVERN] (last visited Feb. 28, 2019).

Generally, economic concern linked to investor confidence is one primary justification for American securities regulation.[160] The prosperity of capital markets and financial communities depends on people being willing to invest, and people are more willing to invest if they have confidence that they are not being taken advantage of.[161] In theory, securities laws signify a commitment to curtailing marketplace abuse, and they add a layer of confidence in investors by mitigating the "fear of exploitation."[162]

After Wall Street crashed in 1929 and many individual investors lost their savings to worthless securities in the postwar decade, investors undoubtedly lost faith in public markets. With the '33 Act, Congress spelled out its chosen remedy—disclosure.[163] Often referred to as the "truth in securities" law, the '33 Act protects investors by requiring companies to fully and fairly disclose important financial information about public offerings of securities during the registration process.[164] Justifying the federal regulatory framework then depends on a core assumption that potential investors will behave rationally and make informed decisions about whether to purchase a company's securities in response to the information they receive.[165]

The Securities Exchange Act of 1934 (the "'34 Act") imposed greater administrative responsibility and extended government reach further into the securities industry. Consequently, Congress established the Securities and Exchange Commission through Section 4 of the Act to address a laundry list of problem areas.[166] The '34 Act covers all aspects of publicly traded securities and also provides actions for market manipulation, insider trading, manipulation concerning the purchase or sale of stock, misstatements among documents filed with the Commission, and various other problems with securities sales, sellers, and buyers.[167] As such, Congress granted the SEC, along with other administrative agencies initiated around this time, broad power to directly regulate through rules, orders, and enforcement.[168] But Congress also enacted a check on the executive branch and these relatively new agencies in 1946 with the Administrative Proce-

160. *See* JAMES D. COX ET AL., SECURITIES REGULATION: CASES AND MATERIALS 5 (Rachel E. Barkow et al. eds., 8th ed. 2017).
161. *See id.* at 4.
162. *Id.* at 5.
163. *See* THE LAWS THAT GOVERN, *supra* note 159.
164. *Id.*
165. *See id.*
166. *See* COX ET AL., *supra* note 160, at 9.
167. *See* THOMAS LEE HAZEN, FEDERAL SECURITIES LAW 4 (Kris Markarian ed., 3d ed. 2011).
168. *See id.* at 5.

dure Act, which gave courts the power to review and invalidate problematic administrative actions.[169]

2. The Division of Enforcement

The SEC is an independent, nonpartisan agency that operates through four main divisions: the Division of Corporation Finance, the Division of Trading and Markets, the Division of Investment Management, and the Division of Enforcement. Because of its ability to investigate and prosecute, the Division of Enforcement gains frequent publicity and is the most prominent of the divisions to the general public.[170] The Division of Enforcement is typically poised to initiate either an administrative proceeding or enforcement action brought in a federal court, or to refer its findings to the Department of Justice for criminal prosecution after investigating.[171]

In October 2008, the Commission made its Enforcement Division manual ("Manual") available for the first time, which lays out all the policies and procedures SEC enforcement officers are to follow while investigating a possible securities violation.[172] But for purposes of this Note, the most relevant process to emphasize is that which officers need to complete to issue a valid subpoena for documents or witnesses pursuant to federal securities laws.[173]

Initially, the SEC begins investigating a possible securities violation based on general market surveillance, investor complaints, media reports, reports from other SEC divisions and offices, or referrals from various other sources.[174] After obtaining enough evidence, the Director of the Division may issue a "Formal Order of Investigation," which describes the nature of the investigation and designates staff members as officers for the purposes of the investigation. Among other things, the designated officer has the power to subpoena witnesses and require document production.[175]

169. *See* 5 U.S.C. §§ 701–06 (2011); Tabaie, *supra* note 127, at 785–86.

170. *See* COX ET AL., *supra* note 160, at 15.

171. *See* HAZEN, *supra* note 167, at 18.

172. *See KEEPING CURRENT: The SEC Enforcement Manual—An aid to combat SEC investigations*, AM. BAR ASS'N (June 29, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2009/03/keeping_current_masella/ [https://perma.cc/CP39-45ES].

173. *See* SEC. AND EXCH. COMM'N DIV. OF ENF'T, ENFORCEMENT MANUAL 41 (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf [https://perma.cc/SYS2-5L89] [hereinafter MANUAL].

174. *See* U.S. SEC. AND EXCH. COMM'N, HOW INVESTIGATIONS WORK, https://www.sec.gov/enforce/how-investigations-work.html [hereinafter HOW INVESTIGATIONS WORK] [https://perma.cc/TSM2-8TX7] (last visited Feb. 28, 2019).

175. MANUAL, *supra* note 173, at 17–18.

C. The SEC has Broad, Discretionary Subpoena Power

The Commission has the power to subpoena any "books, papers, correspondence, memoranda, or other records" that are "relevant or material" to the agency's inquiry.[176] Like other administrative agencies, an SEC subpoena must abide by the requirements laid out in *Powell*.[177] For example, remembering the executive subpoenaed for documents from the hypothetical described in the Introduction, she may object to the agency's subpoena based on constitutional claims or that the Commission overstepped its boundaries in issuing the subpoena. Either objection would come about by bringing a motion to quash the subpoena in federal court. While not the only constitutional claim available, the hypothetical executive could challenge the subpoena under the Fourth Amendment, claiming that one or more of the *Powell* requirements is not satisfied. Taken with *Oklahoma Press*, the Fourth Amendment also requires the SEC's subpoena to be definite enough in breadth and scope.[178]

As stated, the *Powell* standards are extremely easy to enforce, and that holds true for SEC subpoenas. The Commission has discretion in determining the justification for any given subpoena as the agency is the best situated to discern to what legitimate purpose the requested documents relate.[179] Similarly, the relevancy requirement is inconsequential for the SEC as the agency does not have to affirmatively prove the documents requested are relevant; on the contrary, documents must not be "plainly irrelevant."[180] The last two requirements of the Powell test are technical ways to challenge a subpoena, which are seemingly unhelpful to an individual attempting to quash a subpoena based on privacy implications.[181] Consequently, the current law does not provide much protection—much less privacy protection—through the *Powell* standards.

176. 15 U.S.C. § 78u(b) (2015).

177. *See* United States v. Powell, 379 U.S. 48, 57–58 (1964).

178. *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208 (1946) (noting the Fourth Amendment protects against document requests being too indefinite in their description of items to be produced).

179. *See* Sec. Exch. Comm'n v. Brigadoon Scotch Distrib. Co., 480 F.2d 1047, 1053 (2d Cir. 1973) (acknowledging that the SEC must be free from interference when determining whether certain activities fall under its jurisdiction).

180. Sec. Exch. Comm'n v. Arthur Young & Co., 584 F.2d 1018, 1028–29 (D.C. Cir. 1978).

181. *See* Tabaie, *supra* note 127, at 795–97.

IV. CARPENTER WILL SERVE AS A CHECK ON THE SEC'S VAST AUTHORITY TO OBTAIN INFORMATION

As Justice Alito suggests, one possibility after *Carpenter* is a sweeping requirement that all court orders to produce documents containing sensitive information must be supported by probable cause in the future. Certainly, that is an extreme example and would be "revolutionary." For the SEC, Alito's opinion might not be that far-fetched. After all, subpoenas issued by the SEC are functionally similar to a 2703(d) order described above in Part II.C, and the Commission often requests personal information from individuals during investigations that implicates the Fourth Amendment.

Referencing the 2703(d) order under the Stored Communications Act, Justice Alito asserts that "nothing stops [the majority's] logic from sweeping much further."[182] Requiring the court order to produce documents to be supported by probable cause ostensibly imposes the same requirement on grand jury subpoenas and other agencies with the power to issue document-production orders such as the SEC, Federal Trade Commission, Occupational Safety and Health Administration, and others.[183] For the same reason, Justice Kennedy warns that "the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies" are now uncertain.[184]

Mirroring the Government's argument described in Part III.A, SEC subpoenas are often enforced without meeting warrant requirements for the same reasons observed in grand jury subpoenas and many other administrative agencies. SEC subpoenas are minimally intrusive, objectionable by the recipient, and necessary in determining whether a possible violation of the securities laws exists. A valid 2703(d) order under the SCA has similar qualifications and a clearly higher standard to meet than an SEC subpoena conforming to *Powell*. Therefore, in theory, the Court's invalidation of a 2703(d) order compelling disclosure of location information in *Carpenter* would, in turn, invalidate an SEC subpoena requesting personal information akin to CSLI.

Even as part of a corporate entity, the hypothetical executive's privacy rights will be more salient after *Carpenter* when the SEC requests personal information. As the SEC often names both the entity and the individual or individuals in a formal investigation, distinguishing the rights between the

182. Carpenter v. United States, 138 S. Ct. 2206, 2256 (2018) (Alito, J., dissenting).
183. *Id.* at 2247 (Alito, J., dissenting).
184. *Id.* at 2234 (Kennedy, J., dissenting).

two is significant. Courts have done just that and rarely recognize any significant privacy interest in a corporation's own books or other types of business records.[185] That assertion stems back to over 100 years ago when the Court announced in *Hale v. Henkel* that the "corporation is a creature of the State," and thus Congress is appropriately able to investigate a corporation's papers for wrongdoing.[186]

Oklahoma Press made clear that the Fourth Amendment does not protect a corporation or its officers from producing corporate records and that requests for such documents are not actual "searches" under the Fourth Amendment.[187] Therefore, Fourth Amendment requirements—such as probable cause—are not imposed on administrative subpoenas, at least when they seek corporate records.[188]

Shortly after the *Oklahoma Press* decision, the Court further differentiated a corporation's rights from an individual's in *United States v. Morton Salt Co*. Because corporations are not equivalent to individuals in enjoying a right to privacy, neither the Fourth nor Fifth Amendment privileges apply to them.[189] Having both been decided in the corporate rights context, *Oklahoma Press* and *Morton Salt* seemingly carved out a different policy for individuals—one that may have been alluded to in *Carpenter*.

An individual may still be unable to object to producing records such as corporate tax or payroll reports, but there are other types of business records that "implicate[] basic Fourth Amendment concerns about arbitrary government power much more directly."[190] In *Carpenter*, the "business record" Justice Roberts refers to is CSLI, which the SEC could theoretically issue a subpoena for under the ECPA. The Commission would have to comply with the requirements laid out in the statute, the Enforcement Manual, and now *Carpenter*.

In fact, Congress has enacted several statutes that address individual privacy in response to broad agency subpoena power, namely, the Privacy Act of 1974, the Right to Financial Privacy Act of 1978, and the aforementioned Electronic Communications Privacy Act of 1986. The SEC En-

185. *See, e.g.*, United States v. Morton Salt Co., 338 U.S. 632, 651–52 (1950) (concluding that corporations as privileged entities do not enjoy the same rights to privacy as individuals); Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208 (1946) (the Fourth Amendment only protects against requests for corporate records that are too indefinite or irrelevant); Hale v. Henkel, 201 U.S. 43, 74–75 (1906).

186. *Henkel*, 201 U.S. at 74–75 (1906). *But see* Burwell v. Hobby Lobby Stores, Inc., 573 U.S. 682, 707–08 (2014) (concluding that a closely-held corporations is a "person" under the Religious Freedom Restoration Act).

187. *See* 327 U.S. at 195–96, 202.

188. *See id.* at 209–10.

189. *Morton Salt Co.*, 338 U.S. at 652.

190. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

forcement Manual details how the Commission and its officers should comply with all of these when requesting personal information from the public, banking information, or records of electronic communications.[191] Notably, an individual customer has a privacy interest in financial records held by a bank under the RFPA, but regulated entities such as broker-dealers or investment advisers are not afforded that same protection. Similarly, email communications are protected under the ECPA when stored with third parties, but the ECPA does not extend to email communications stored on a company's internal servers or communications held directly with the sender.[192]

The *Carpenter* holding implies that CSLI is just one example of a business record embodying the "modern-day equivalent of an individual's own 'papers' or 'effects.'" In *United States v. Warshak*, the Sixth Circuit gave an illustrative analysis of Fourth Amendment protections in a modern world, holding that a CEO had a subjective expectation of privacy in the contents of his emails and that expectation was one society would deem reasonable.[193] There, the Government seized around 27,000 emails from the CEO's internet service provider pursuant to the SCA. The CEO's email accounts were critical for business communications, but they also contained his "entire personal life."[194] Because of the sensitive and sometimes incriminating information contained in the emails, the court concluded the CEO clearly expected the contents of his emails to remain private.[195]

Turning to the second prong of the *Katz* reasonableness test, the court emphasized email's prominence in today's modern communication and how individuals frequently and easily send sensitive information to others.[196] Access to an individual's email may uncover business information "relevant" to the government's or an agency's inquiry, but access would also allow government officials or investigators a keen look into an individual's personal life and activities.[197] The Fourth Amendment protects

191. *See* MANUAL, *supra* note 170, at 79–81 (discussing compliance with the Privacy Act, Right to Financial Privacy Act, and Electronic Communications Privacy Act).

192. *Id.* at 81.

193. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

194. *Warshak*, 631 F.3d at 283–84.

195. *See id.* at 284.

196. *Id.* at 284 ("Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button").

197. *See id.*

other traditional forms of communication, and those protections should not dissipate on account of advancing technology.[198]

Although *Warshak* involved a third-party service provider, the holding still signifies important privacy protections in personal information for individuals involved with a business's operations. The court recognized a privacy right in sensitive information, even though such information was blended with business communications that were undoubtedly "relevant" to the fraud investigation. Taken with *Carpenter*, courts have begun showing the willingness to expand and flex the Fourth Amendment to protect the privacy of sensitive digital information.

V. THE HYPOTHETICAL HEDGE FUND EXECUTIVE HAS VIABLE FOURTH AMENDMENT CLAIMS

In *Carpenter*, Justice Roberts assures the Government and administrative agencies that the subpoena will still be available to them "in the overwhelming majority of investigations."[199] Certainly, *Carpenter* does not overrule the *Powell* standards or render them inapplicable in enforcing most subpoenas. But when an individual is faced with an SEC subpoena requesting documents that are either purely personal or personal comingled with business documents, *Carpenter* allows a Fourth Amendment objection to producing those documents—even if the documents are relevant to the Commission's inquiry. Of course, courts must decide whether *Carpenter's* reasoning covers sensitive and intimate information unrelated to location. That seems likely as the Court condemned Justice Alito's view that prescribed a "categorical limitation on the Fourth Amendment."[200] In other words, agencies and grand juries should not be able to circumvent the warrant requirement in obtaining personal documents such as "private letters" and the "digital contents of a cell phone" based on nothing more than "official curiosity" behind a subpoena.[201]

For the hypothetical executive referenced above, she ought to bring a motion to quash the SEC's subpoena, at least with regard to her personal smartphone and emails. Information gleaned from those two sources may be relevant to the SEC's investigation, but they are both wrought with privacy concerns approaching the same level as CSLI.[202] Under *Warshak*,

198. *See id.* at 285 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001) (advancing technology should not be allowed to "erode the privacy guaranteed by the Fourth Amendment").

199. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

200. *Id.*

201. *Id.*

202. *See id.*

accessing the executive's emails may require a warrant, especially if she does not have separate business and personal accounts. Accessing the executive's smartphone, however, would almost surely require the SEC to obtain a warrant supported by probable cause. Indeed, the Supreme Court in *Riley v. California* recognized that modern cell phones are capable of storing vast amounts of sensitive information and the "privacies of life."[203]

That phenomenon raises privacy concerns comparable to CSLI, but potential problems do not lie exclusively with a cell phone's storage capacity. Smartphones give people abilities they have never had before with the touch of a finger, from paying virtually any bill to linking their diet or weight-monitoring program to their Fitbit. All of these examples raise privacy concerns at least as salient as those associated with CSLI, and someone like the hypothetical executive should not forgo her privacy because she wants to use modern capacities. Therefore, with the *Carpenter* Court's approval of both *Warshak* and *Riley*, a greater level of scrutiny ought to be applied to administrative subpoenas requesting such personal information—the "reasonable relevancy" standard combined with the *Powell* requirements will not suffice.

For the SEC, such an implication means the Commission may need to reconsider for which types of records it issues subpoenas and for which types of records the agency obtains a warrant. If anything, the officers drafting a subpoena should do so more carefully, focusing on documents that are clearly not private.[204] A more precise subpoena would mitigate any potential litigation over subpoena enforcement for private documents, which seems to be a heavier consideration after *Carpenter*. The Commission could also develop an internal review board, separate from the investigators, that looks for material which is protected.

Undoubtedly, SEC regulated entities must assure they have an adequate compliance system in place, especially with policies and procedures to address the production of business and personal documents.

CONCLUSION

The need for investor protection and proper market regulation has not waned in the past years, and *Carpenter* should certainly not be interpreted in a way that hinders the investigative abilities of the SEC, grand juries and

203. Riley v. California, 573 U.S. 373, 403 (2014) (quoting Boyd v. United States, 116 U.S. 616, 625 (1886)). In *Riley*, police officers' safety did not justify ridding of the warrant requirement when searching through an arrestee's cellphone. *See id.* at 401.

204. *See* Tabaie, *supra* note 127, at 816.

other administrative agencies alike. However, as American citizens become more attached to and intertwined with their devices, the Supreme Court has highlighted the tenuous balance between regulatory efficiency and constitutional protections. Rather than allowing agencies such as the SEC to demand documents based only on "official curiosity," more scrutiny ought to be applied to document requests implicating private documents, especially as more people rely on modern technology for myriad purposes today. While technological advances have convoluted the Fourth Amendment privacy doctrine and created concerns the Framers could never have imagined, the sheer difficulty or complexity in enforcing constitutional rights is no reason to abandon them altogether.