"THIS MEETING IS BEING RECORDED": 'ZOOM'-ING AWAY FROM THE THIRD-PARTY DOCTRINE

*Marcus Schlundt Bodien**

ABSTRACT

Videoconferencing arguably became one of the most useful but pervasive features of the pandemic. Given how pleased institutions are with recent productivity, statistics show use of these platforms is unlikely to disappear or even substantially diminish once the public health landscape fully recovers. As such, society faces an entirely new consideration: How and to what extent is the data collected by videoconferencing platforms protected from government access? And, what control, if any, do we as individuals retain over such data?

The third-party doctrine, which concerns itself with ownership rights of information voluntarily passed to third parties, generally diminishes an individual's rights and expectations of privacy regarding data collected by third parties. However, the Court incepted the doctrine long before the World Wide Web was released, and modern developments to the doctrine place the expectation of digital privacy on unstable ground. Whatever the case may be, the individual—compelled to use videoconferencing platforms by academic and employment institutions—is not, in any formal sense, voluntarily conveying information to third parties in the manner traditionally understood to implicate the doctrine. Thus, the data collected by videoconferencing platforms should fall outside the scope

* Marcus is a third-year law student at the Drexel University Thomas R. Kline School of Law, graduating Spring 2022. His interests include the study of American Philosophy, specifically focusing on Pragmatism which, in part, seeks to track meaning and practical consequences that flow from language and argument. Upon graduation, Marcus plans to practice representing plaintiffs in employee rights disputes. This Note focuses on a combination of those interests and traces the pragmatic effects that the recent Supreme Court of the United States decision in *Carpenter v. United States* has on employees, academics, and professionals through the lens of data privacy. Thank you to Lily and Quinn for being my inspiration, Carley for your unwavering support, and to Dr. Andrew Howat for sharing your academic expertise with me.

of the third-party doctrine and should likewise require the government to obtain a warrant to access the data chronicled as a product of institutionally mandated videoconferencing platform use.

TABLE OF CONTENTS

INTRODUCTION

Our lives changed these past years. Many of us interact with the world through the four corners of our computer screens now more than ever—and this virtual environment is likely to subsist.[1] As the world charts new digital landscapes, we are

1. *See* Denisa R. Superville, *Remote Learning Will Keep a Strong Foothold Even After the Pandemic, Survey Finds*, EDUC. WK. (Dec. 15, 2020) https://www.edweek.org/leadership/remote-learning-will-keep-a-strong-foothold-even-after-the-pandemic-survey-finds/2020/12; Anne Dennon, *Half of Remote College Students Plan to Stay Online Post-Pandemic*, BESTCOLLEGES (May 20, 2021), https://www.bestcolleges.com/research/remote-college-students-stay-online-post-pandemic ("Most college students will have the option to continue learning remotely for the foreseeable future . . . [and] nearly half of all students surveyed said they were likely to engage in online (49%) or remote (48%) learning even after colleges resume normal operations.").

contained, even compelled, to these spaces now more than ever. Fortunately, we are able to carry on productivity in many capacities—compared to the 1918 pandemic, where businesses and schools closed for up to four months without effective means to communicate.[2] But it would be imprudent to consider the results of today's public health landscape as a one-off. That is, research shows that, whether by choice or obligation to comply with public health mandates, 67% of companies expect work-from-home to be permanent or long lasting.[3] Additionally, projections show, and experts agree that, "25% of all professional jobs in North America will be remote by the end of 2022, and remote opportunities will continue to increase through 2023."[4]

Thus, moving ahead, we are poised to carry our means of social productivity forward by broadcasting ourselves in innovative ways, specifically in academic and professional spheres. Thankfully, anchorage points in digital meeting platforms, such as Zoom, provide us with the capability to broadcast channels of communication, and have no doubt made our transitions to digital communication more practical. But pay attention to the robotic prompt as you activate your audio: "This meeting is being recorded."[5] *Are we sacrificing any privacy interest whenever we log in to the virtual space?* Whether for a work

2. *See* Mary Battenfeld, *3 Lessons from How Schools Responded to the 1918 Pandemic Worth Heeding Today*, THE CONVERSATION (June 16, 2020, 7:52 AM), https://theconversation.com/3-lessons-from-how-schools-responded-to-the-1918-pandemic-worth-heeding-today-138403.

3. *See* Annie Pilon, *67% of Companies Expect Work from Home to Be Permanent or Long-Lasting*, SMALL BUS. TRENDS, https://smallbiztrends.com/2020/06/work-from-home-permanently-survey.html (July 22, 2020). Moreover, 94% of businesses report higher productivity with use of videoconferencing platforms, which indicates the continued use of such platforms. *See* Lewis Keegan, *Video Conferencing Statistics (All You Need to Know!)*, SKILLSCOUTER, https://skillscouter.com/video-conferencing-statistics/ (Aug. 4, 2021).

4. Bryan Robinson, *Remote Work is Here to Stay and Will Increase into 2023, Experts Say*, FORBES (Feb. 1, 2022, 6:24 AM), https://www.forbes.com/sites/bryanrobinson/2022/02/01/remote-work-is-here-to-stay-and-will-increase-into-2023-experts-say/.

5. This prompt is pre-recorded and delivered in Zoom meetings when the meeting host begins recording. *Providing Consent to be Recorded*, ZOOM, https://support.zoom.us/hc/en-us/articles/360061691631 (Dec. 10, 2021).

meeting, a classroom setting, or a virtual social gathering, we are exposed to new considerations of privacy, albeit not in totally new ways, but in ways that American jurisprudence lags behind.

Historically, the government can access personal data without a warrant whenever an individual voluntarily relinquishes data to a third party.[6] This accessibility is known as the third-party doctrine.[7] The general rationale is that an individual loses any reasonable expectation of privacy when information is voluntarily provided to a third party, as the individual assumes the risk that the data, in possession and ownership of the third party, may be shared—thereby nullifying the need for a search warrant.[8] This rationale begs the question in today's virtual world: Do employees, students, and professors, using platforms like Zoom, voluntarily assume the risk in the same way that the third-party doctrine has traditionally been understood to apply? In a formal sense, we voluntarily choose to work, and we choose to pursue our education, at least beyond high school.[9] But, do we *per se* voluntarily convey personal data about ourselves when we enter the virtual classroom or employment setting? Put simply, are we the ones actually providing information to these third parties?

This Note argues that, in light of recent confusion concerning the third-party doctrine, students and employees should retain a reasonable expectation of privacy of data conveyed over videoconferencing platforms because the information is collected incidentally as a byproduct of institutionally mandated use; thus, such individuals are not voluntarily

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

7. *See generally id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)) (describing *Smith* and its progeny's establishment of this doctrine).

8. *See id.* at 745.

9. Questions encompassing the freedom of employment in American culture are not at issue here. Instead, this Note assumes that employment is a condition of American culture.

utilizing digital meeting platforms in ways traditionally understood to implicate the third-party doctrine.[10] For the purposes of argument, this Note narrows the discussion to the academic and employment context of videoconferencing, though there is room for debate surrounding the voluntariness of casual social functioning and the expectations of privacy concerning those realms of protection. Zoom is used as the anchor for discussion, as it has become the most prevalent conferencing platform.[11] As such, Zoom's privacy policy[12] is the reference for discussion; however, any institution compelling students or employers to use a particular videoconferencing platform should maintain the expectation of privacy regardless of the specific platform utilized.[13]

Part I of this Note examines the background to the Fourth Amendment doctrine, the development of the third-party doctrine, and its recent changes. Part II explores issues regarding clarity and ambiguities resulting from recent changes to the third-party doctrine and how to proceed with the doctrine moving forward. Part III presents the Zoom privacy policy, what information the company collects, and Zoom's current commitments to privacy. Finally, Part IV demonstrates how lower courts have struggled with recent changes to Fourth Amendment doctrine and argues that the data collected by Zoom should not apply to the third-party doctrine, as there is a reasonable expectation of privacy to our endeavors over videoconferencing platforms today.

10. *See Smith*, 442 U.S. at 743.

11. *See* Mansoor Iqbal, *Zoom Revenue and Usage Statistics (2021)*, BUS. OF APPS, https://www.businessofapps.com/data/zoom-statistics/ (Nov. 11, 2021). Zoom reported more than 300 million daily users as of April 2020 and was only one of three apps to have been installed over 300 million times in a single quarter. *Id.*

12. *Zoom Privacy Statement*, ZOOM, https://zoom.us/privacy (Nov. 1, 2021).

13. For example, applications include Microsoft Teams, Google Meet, FaceTime, etc. *See Privacy Cannot Be a Casualty of the Coronavirus*, N.Y. TIMES (Apr. 7, 2020), https://www.nytimes.com/2020/04/07/opinion/digital-privacy-coronavirus.html;
Kate O'Flaherty, *Zoom Alternatives: 5 Options for People Who Care About Security and Privacy*, FORBES (Apr. 4, 2020, 10:15 AM),
https://www.forbes.com/sites/kateoflahertyuk/2020/04/04/zoom-alternatives-5-options-for-people-who-care-about-security-and-privacy.

I. BACKGROUND

An understanding of the potential privacy concerns implicated by Zoom and other digital meeting platforms requires a brief history of the development of Fourth Amendment protections.

A. *The Fourth Amendment and the Third-Party Doctrine*

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[14]

Traditionally, Fourth Amendment rights focused on protections against *physical* intrusions, which generally encompassed trespass upon property rights.[15] However, in 1967 the Supreme Court in *Katz v. United States* recognized an expansion of Fourth Amendment jurisprudence when it held "the Fourth Amendment protects people, not places."[16] That is, the Court moved away from the old doctrine, which exclusively considered physical intrusions on constitutionally protected areas, and instead stated: What a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[17]

14. U.S. CONST. amend. IV.

15. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) ("For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' and focused on whether the Government 'obtains information by physically intruding on a constitutionally protected area.'" (quoting United States v. Jones, 565 U.S. 400, 405–06 n.3 (2012))).

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

17. *Id.*; *see also* Silverman v. United States, 365 U.S. 505, 511–12 (1961) (holding that the Fourth Amendment extends to the recording of oral statements without a technical trespass to property).

In *Katz*, the Court specifically considered whether conversations held in a public phone booth were subject to warrant requirements.[18] The Government placed recording devices on the outside of the booth that listened in on conversations taking place inside.[19] The Government argued that because there was no property interest trespassed upon, there was no Fourth Amendment violation.[20] However, in recognizing the technological advancements of electronic recordings, the Court adopted the "reasonable expectation of privacy" test to determine whether the Government had conducted a search under the meaning of the Fourth Amendment, thereby implicating the amendment's protection.[21] The test considers: (1) whether the individual's conduct exhibits "an actual (subjective) expectation of privacy," and (2) whether the individual's expectation of privacy is objective, or, "one that society is prepared to recognize as 'reasonable.'"[22] The Court concluded the petitioner in *Katz*, though in public, entered a phone booth and closed the door not to shield himself from the prying eye, but the "uninvited ear."[23] As such, he did not "shed his right[s]" merely by appearing in public, and that when he entered the phonebooth, shut the door, and paid the toll, he was "surely entitled to assume that the words he utter[ed] . . . [would] not be broadcast to the world."[24] The Court has since clarified that *Katz* enlarged the Fourth Amendment's sphere to include not only the traditional common law trespass protections, but also a person's reasonable expectation of privacy.[25]

18. *Katz*, 389 U.S. at 349.

19. *Id.* at 348.

20. *Id.* at 352–53.

21. *Id.* at 360 (Harlan, J., concurring).

22. Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing *Katz*, 389 U.S. at 361) (Harlan, J., concurring)).

23. *Katz*, 389 U.S. at 352 (setting the jurisprudence standard for what constitutes a "search").

24. *Id.*

25. *See* United States v. Jones, 565 U.S. 400, 407–09 (2012).

However, privacy interests narrow when a person transmits information to a third party.[26] As mentioned previously, the third-party doctrine states that we forfeit our reasonable expectation of privacy upon voluntarily relinquishing information to third parties.[27] In both *Smith v. Maryland*[28] and *United States v. Miller*,[29] the Court invoked a property theory of Fourth Amendment jurisprudence, holding that the defendants had no legitimate expectation of privacy to phone records stored in pen registers nor in checks exchanged at a bank during normal business dealings.[30] The Court stated that when individuals convey information to a third party, they essentially give up control and ownership of that information.[31] As such, the information held by the third party effectively belongs to the third party as opposed to the individual; and, in the event the government seeks to access such information, the issue is between the government and the third party, not the individual who originally possessed the information.[32]

Property interests aside, the Court in *Smith* and *Miller* also elucidated the individuals' actions to determine whether they had a reasonable expectation of privacy independent of ownership.[33] The Court clarified that because the defendants "assumed the risk" that the third party could convey the information to the government, there was no objective expectation of privacy.[34] That is, the defendants voluntarily

26. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

27. *See id.* (citing *Smith*, 442 U.S. at 743–44).

28. *Smith*, 442 U.S. at 745–46.

29. United States v. Miller, 425 U.S. 435, 442–43 (1976).

30. *Id.*; *Smith*, 442 U.S. at 745–46.

31. *See Smith*, 442 U.S. at 743–45.

32. *See id.* at 744 (quoting *Miller*, 425 U.S. at 443).

33. *Id.*; *Miller*, 425 U.S. at 442–43.

34. *Smith*, 442 U.S. at 744; *see also Miller*, 425 U.S. at 443. The Court also considered the nature of the documents in both cases. In *Smith*, it concluded that pen registers have limited capabilities, and that call logs reveal little identifying information. *Smith*, 442 U.S. at 741–42 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)). In *Miller*, the Court noted that checks are "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442. *But see* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding that cellphones, because they are able to track a person's physical movements simply by being turned on and thus allow for physical location data to be

provided phone numbers to the telephone company and negotiable bank documents to bank tellers in the normal course of business.[35] And, even in the event there was an assumption that the information would be used for a limited purpose, Courts have long held that the "Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."[36]

B. *Modern Third-Party Doctrine Concerns: Enter Carpenter*

More than five decades after the creation of the third-party doctrine, the Supreme Court created an overdue exception. The Court in *Carpenter v. United States* focused on contemporary use of technological advancements and its entry into our private spheres to reframe the third-party doctrine, noting technology's essential but invasive role in our daily functioning.[37]

The *Carpenter* Court determined that cell-site location information ("CSLI"), which produces time-stamped general location records stored with cellphone carriers, was not excluded from Fourth Amendment protection under the third-party doctrine and therefore required a warrant.[38] The Court explained that CSLI essentially works by sending a signal from a person's cellphone to a nearby cell tower to route calls, text messages, and similar forms of communication.[39] As a result, each cellphone accesses the cell site to triangulate location and cellphone companies then keep this information, which in turn allows the companies to determine the general location of the cellphone when a call is placed.[40]

In this case, the Court considered the collection of 127 days' worth of location cataloging, which yielded 12,898 triangulated

"compiled every day, every moment, over several years," implicate privacy concerns that extend far beyond *Smith* and *Miller*).

35. *Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 442.

36. *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 442).

37. *See Carpenter*, 138 S. Ct. at 2216–17.

38. *Id.* at 2211, 2221.

39. *Id.* at 2211–12.

40. *Id.* at 2211–12, 2219.

location positions of the defendant—an average of 101 location points per day.[41] The defendant sought to suppress the CSLI data, which placed him near the location of multiple robberies for which he was being investigated.[42] The trial court denied the motion to suppress, and the Sixth Circuit affirmed, holding that Carpenter did not have a reasonable expectation of privacy in information that he shared with the cellphone company.[43] The Supreme Court granted certiorari and analyzed the case from two perspectives: (1) the individual's expectation of privacy in his physical locations, and (2) the applicability of the third-party doctrine.[44] Both lines of reasoning provide valuable insight and support the ultimate conclusion that the third-party doctrine should not apply to Zoom or other videoconferencing applications.[45]

Concerning the individual's expectation of privacy, the Court reiterated that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[46] In this particular case, the government was able to collect the data conveyed by CSLI through the Stored Communications Act, [47] which required a subpoena or court order for release of such information, as opposed to a warrant.[48]

41. *Id.* at 2212.

42. *Id.* at 2212–13.

43. *Id.*

44. *See id.* at 2214–16.

45. *See generally id.* at 2213–14 (discussing the evolution of the Fourth Amendment in the context of protecting the privacy of individuals in an era of rapidly advancing technology).

46. *Id.* at 2217 (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)).

47. *Id.* at 2212. The "statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id.* (quoting Stored Communications Act, 18 U.S.C. § 2703(d)).

48. *See id.* The touchstone of a warrant is probable cause. *Id.* at 2221. Probable cause requires a standard considering the totality of the circumstances to determine whether there is fair probability that either a person has committed a crime, is about to commit a crime, or that evidence relevant to a crime exists in a particular location. *See* Illinois v. Gates, 462 U.S. 213, 236–39 (1983). This standard deals in probabilities. *See id.* Moreover, a mere conclusory statement that gives the magistrate virtually no basis for making a judgment regarding probable cause is insufficient. *Id.* at 239. The totality of the circumstances test satisfies the need for a magistrate's "substantial basis" for concluding a search will uncover evidence of wrongdoing.

Furthermore, the Court reiterated that individuals have a reasonable expectation of privacy "in the whole of their physical movements" with respect to GPS tracking.[49] As such, the Court stated that prior to the digital age, law enforcement could have tracked the physical movements of individual's for only brief amounts of time.[50] However, these traditional methods of tracking that extended a number of days would become too costly and difficult.[51] Therefore, society recognizes the expectation that law enforcement would not "secretly monitor and catalogue every single movement of an individual . . . for a very long period."[52] The Court held that access to cellphone location records contravened society's expectation of privacy,[53] specifically because a cellphone "faithfully follows its owner beyond public thoroughfares and into private residences."[54]

The Court then discussed several considerations regarding the pervasiveness of cellphone location tracking, noting the vital role cellphones place in society today.[55] CSLI logs location information for all 400 million cellphone users in America.[56]

See id. at 238–39. On the other hand, the Supreme Court has specifically required *only* that a "subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." Donovan v. Lone Steer, Inc., 464 U.S. 408, 415 (1984) (quoting See v. Seattle, 387 U.S. 541, 544 (1967)).

49. *See Carpenter*, 138 S. Ct. at 2217–18 (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).

50. *Id.* at 2217.

51. *Id.*

52. *Id.* This begs the question as to whether society's expectation of privacy could change with the digital age. That is, this presupposition by the Court raises the rhetorical question of whether police practices will adjust to a shift in society's normative interpretation of what constitutes "reasonable" monitoring of location information, given such regular use of technology.

53. *Id.*

54. *Id.* at 2218.

55. *Id.* Although Chief Justice Roberts does not mention these factors outright in his majority opinion, Justice Kennedy outlined these factors as flowing from the Chief Justice's argument and Justice Kennedy then expressed concern that the relative weight for each factor remained undisclosed, thus creating confusion for future application of Fourth Amendment law; the factors include "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness." *Id.* at 2234 (Kennedy, J., dissenting).

56. *Id.* at 2218 (majority opinion).

Thus, this new tracking method does not just follow individuals who may come under investigation, but applies to every American carrying a cellphone.[57] The Court further reasoned that unlike GPS tracking, which the Court already held was an unreasonable search,[58] this type of tracking did not require police to know prospectively whether they wanted to follow a particular person.[59] Instead, the CSLI records are available for retroactive access and inquiry.[60] And, "[o]nly the few without cellphones" would be able to escape the purview of "absolute surveillance."[61] As such, the Court held that regarding the Stored Communications Act, cellphone users retain a reasonable expectation of privacy with respect to as little as seven days' worth of data conveyed by CSLI.[62]

Concerning the third-party doctrine, the Court provided that cellphones play a unique role in society's functioning.[63] Further, merely possessing a cellphone that relays location information to the cell company's database does not cause the individual to surrender all Fourth Amendment protections under the third-party doctrine.[64] That is, for the Court in *Carpenter*, the fact that an individual did not *own* the information shared with a third party "[did] not negate [the individual's] anticipation of privacy in his physical location."[65] As such, the Court noted that the government's request extended beyond the third-party doctrine—stating that, although privacy interests are diminished due to a lack of reasonable expectation of privacy, Fourth Amendment protections do not simply drop out of the frame when something is shared with a third party.[66]

57. *Id.*
58. *See* United States v. Jones, 565 U.S. 400, 404 (2012).
59. *Carpenter*, 138 S. Ct. at 2218.
60. *Id.*
61. *Id.*
62. *Id.* at 2217.
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.* at 2219.

The Court also distinguished the information gathered in *Smith* and *Miller,* stating there was a "world of difference" in the ability to ascertain location records by a cellphone company revealing its customer's movements dating back years.[67] Regarding both *Smith* and *Miller*, the *Carpenter* Court considered the nature of the information shared with a third party.[68] It came to the conclusion that pen registers have limited capabilities, and that call logs reveal little "identifying information."[69] Further, checks are "not confidential communications but negotiable instruments to be used in commercial transactions."[70] On the other hand, cellphone locations collected by carriers portray an "exhaustive chronicle of location information casually collected by wireless carriers."[71] That is, cellphones are able to track a person's physical movements simply by powering the phone on—and require no more intentional effort to track a user's data.[72] Thus, CSLI allows for a compilation of physical presence "compiled every day, everyone moment, over several years" and consequently implicates privacy concerns extending far beyond *Smith* and *Miller*.[73]

Finally, the Court noted that the third-party doctrine's rationale concerning voluntary relinquishment by the individual does not square with respect to CSLI.[74] The Court stressed that the location information was not shared in the way one normally understands the word, stating, "a cell phone logs a cell-site record by dint of its operation, without any *affirmative act* on the part of the user beyond powering up."[75] Further, nearly all phone functionalities generate CSLI, including

67. *Id.*

68. *See id.*; Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

69. *Carpenter*, 138 S. Ct. at 2219 (quoting *Smith*, 442 U.S. at 744).

70. *Id.* (quoting *Miller*, 425 U.S. at 442).

71. *Id.*

72. *See id.* at 2217–19.

73. *Id.* at 2220.

74. *Id.*

75. *Id.* (emphasis added).

"incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates."[76] Lastly, the Court stated that cellphones are a pervasive and indispensable tool used in modern society and that the only way to avoid leaving a trail of location data is to disconnect from the network.[77] As such, the Court distinguished CSLI from other third-party doctrine cases, holding that the user did not voluntarily "assume the risk" of turning over "a comprehensive dossier" of user information.[78]

Although the Court in *Carpenter* provided limitations to the doctrine, Chief Justice Roberts was careful to conclude his opinion by stating:

> Our decision today is a narrow one. We do not express a view on matters not before us . . . . We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.[79]

II. *CARPENTER*'S CONFINEMENT: A LACK OF CLEAR GUIDANCE

Carpenter carved out an exception to the formal third-party doctrine, but its reasoning and holding left the parameters of its scope open to interpretation.[80] The Court provided a necessary constraint to the third-party doctrine, because the doctrine, as it stood, was poised to potentially exploit individual privacy attached to passively conveyed data.[81] The majority relied on a number of factors when it reached its holding, without ever

76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *See supra* Part I.
81. *See supra* Part I.

formally outlining those factors or stating each factor's relative weight or importance.[82] Now, *Carpenter* sets an unstable foundation for its progeny, essentially begging the question as to what lower courts should do when faced with a potentially novel implication to privacy: (1) What remains within the parameters of the traditional third-party doctrine; and (2) how do we now gauge a reasonable expectation of privacy when utilizing technology that possesses a "unique nature" in our social functioning?[83] *Carpenter*'s facts outlined the distinctive role cellphones play in society, confirming that they are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.'"[84] However, unless technological advancements come to a grinding halt, *Carpenter* is not the last the Court will see of "indispensable" technology questioning our reasonable expectation of privacy.[85]

As stated earlier, 67% of companies expect at-home work to persist and employment projections show remote work continuing for the foreseeable future.[86] Simultaneously, Zoom has seen its customer base rise from 10 million users a day in 2019 to nearly 300 million users per day by June 2020.[87] Compare these statistics to those motivating the reasoning in *Carpenter* and one can recognize the remaining ambiguities that the Court could have clarified.[88] That is, the Court expressly stated that "because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against

82. *See generally Carpenter*, 138 S. Ct. at 2221. Instead, Justice Kennedy outlined these factors in his dissent and expressed concern for confusion and lack of clarity for application by law enforcement. *See id.* at 2234 (Kennedy, J., dissenting).

83. *See id.* at 2266–67 (Alito, J., dissenting).

84. *Id.* at 2220 (majority opinion) (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

85. *See id.* at 2266–67 (Alito, J., dissenting).

86. *See* Pilon, *supra* note 3; Castrillon, *supra* note 4.

87. Iqbal, *supra* note 11.

88. Although public health crises are unprecedented, of course, this critique is more of an expansion of technological advancements playing a role in our daily functioning, to the extent that such use butts up against our constitutional rights.

everyone."[89] Zoom is trending in the same direction—Zoom's 300 million users are on par with the pervasive use of cellphones.[90] And, although Zoom is not engaged at all hours of the day, Zoom similarly tracks not only a user's location but other revealing data.[91] Zoom is available for use on any computer or smart phone when accessed through its app; thus, broadening the potential analogs for tracking compared to the cellphones in *Carpenter*.[92] Furthermore, when utilized in employment or academia, a user is likely to use the platform at any point during the average eight-hour work day or similarly lengthy academic duration including classes, projects, and other school-related meetings.[93] It is no question that the third-party doctrine is outdated, which *Carpenter* presumably recognized, but the holding did not go far enough to offer clear guidance on Fourth Amendment protections.[94] *Carpenter*'s narrow holding has left lower courts confused and without direction.[95]

These concerns bring us to what the *Carpenter* Court should have outlined more clearly. Chief Justice Roberts did the public a service by carving out an exception to the third-party doctrine, but his majority opinion did little to actually narrow the doctrine.[96] Chief Justice Roberts delivered a narrow opinion, but he should have instead provided clearer guidelines on how to approach the doctrine in the future.[97] Cellphones are certainly a pervasive and essential tool that have the capability of permeating individuals' more private spheres, but they are

89. *See Carpenter*, 138 S. Ct. at 2218.

90. *See* Iqbal, *supra* note 11.

91. *Zoom Privacy Statement*, *supra* note 12.

92. *See id.*

93. The average Zoom meeting lasts anywhere from thirty-one to sixty minutes. Keegan, *supra* note 3. With 300 million daily users, that, of course, means that there is an average of 150–300 million hours of Zoom video minutes logged on any given day. *See id.*; Iqbal, *supra* note 11.

94. *See supra* text accompanying notes 63–79.

95. *See infra* Part IV.

96. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

97. *See id.*

certainly not the only technology or device capable of such intrusion.[98]

In his dissent, Justice Kennedy, on the other hand, nicely articulated these concerns flowing from the majority opinion.[99] He was correct to note that the majority's holding offers "no indication [of] how to determine whether any particular category of information falls on the [traditional *Miller*] financial-records side or the cell-site-records side of [the third-party doctrine's] newly conceived constitutional line."[100] He noted that the majority's multifactor analysis considered: (1) intimacy,[101] as CSLI data revealed intimate details about persons' actions as they move from one location to the next;[102] (2) comprehensiveness,[103] as police are able to comprehensively "monitor and catalogue" movements of individuals utilizing cellphones for a long periods of time;[104] (3) police expenses,[105] as investigative costs were significantly lessened when compared to traditional investigative methods;[106] (4) retrospective searches,[107] as CSLI data is available in hindsight, such that, "[u]nlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when[;]"[108] and (5) voluntariness,[109] as cellphone users carry phones compulsively and do not voluntarily share location data with cellphone companies in ways the word voluntary is traditionally understood.[110]

Justice Kennedy was correct to note these concerns, but there is still work to be done to solidify a new third-party doctrine

98. *See id.*
99. *Id.* at 2234 (Kennedy, J., dissenting).
100. *See id.*
101. *Id.* at 2234.
102. *Id.* at 2217–18 (majority opinion).
103. *Id.* at 2234 (Kennedy, J., dissenting).
104. *Id.* at 2217 (majority opinion).
105. *Id.* at 2234 (Kennedy, J., dissenting).
106. *Id.* at 2217–18 (majority opinion).
107. *Id.* at 2234 (Kennedy, J., dissenting).
108. *Id.* at 2218 (majority opinion).
109. *Id.* at 2234 (Kennedy, J., dissenting).
110. *Id.* at 2220 (majority opinion).

moving forward. Although the majority supported its argument relying on these factors,[111] Justice Kennedy was quick to note the ambiguity regarding the relative weight each factor should get, if at all.[112] Justice Kennedy correctly concluded by saying such ambiguity places the "law on a new and unstable foundation."[113]

The Court has long struggled to articulate where the line is drawn when considering whether a reasonable expectation of privacy exists.[114] Over three decades ago, the Court in *Oliver v. United States* stated that "[n]o single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion."[115] What society considers a reasonable search in light of technological advancements has undoubtedly changed, with which both the majority and dissenting opinions in *Carpenter* agree.[116] However, the question of where to draw the line still remains.

Fourth Amendment jurisprudence and doctrine could benefit from a modified factor analysis of the *Carpenter* majority. As a result, the doctrine would broaden the scope of the *Carpenter* holding to include videoconferencing platforms that have become such an involuntary part of our social functioning that they should require a warrant for government apprehension.[117] Furthermore, though issues surrounding the third-party doctrine may still persist, the factors utilized in the majority and the concerns expressed in the dissent may both support the finding that protecting videoconferencing data today is sufficiently analogous to the reasoning that supports protecting

111. *See id.* at 2217–18, 2220.

112. *See id.* at 2234 (Kennedy, J., dissenting).

113. *Id.*

114. *See* Oliver v. United States, 466 U.S. 170, 176–77 (1984).

115. *Id.* at 177.

116. *See Carpenter*, 138 S. Ct. at 2217–20; *id.* at 2234 (Kennedy, J., dissenting).

117. *See id.* at 2234 (Kennedy, J., dissenting) (discussing the difficulty of distinguishing "categor[ies] of information" and the applicability of the third-party doctrine).

CSLI, and should thus be exempt from the third-party doctrine.[118]

Again, we are impelled to these virtual spaces. And, predicated upon the "new normal" and institutional restructuring, society will continue to communicate through digital platforms.[119] Thus, despite our best efforts, where and when we speak to each other over these platforms may become subject to search without traditional protections under the Fourth Amendment. We, in many cases, could not prevent data regarding our personal or professional endeavors from potential warrantless government intrusion simply because the act of conveying information to third parties does not traditionally generate privacy rights.[120] Thus, four factors should maintain from the *Carpenter* majority: (1) intimacy; (2) comprehensiveness; (3) retrospectivity; and (4) voluntariness.[121] In this way, the majority opinion is preserved but broadened beyond the context of its narrow holding merely concerning cellphone data; and thus, the limitations of the third-party doctrine are extended.[122] Additionally, clarity in the doctrine would alleviate the dissent's concern for uncertainty and would resolve issues applying the doctrine in the future.[123]

118. *See id.* at 2217–20 (majority opinion); *id.* at 2234 (Kennedy, J., dissenting).

119. *See* Tim Bajarin, *Work from Home Is the New Normal for Workers Around the World*, FORBES (Apr. 29, 2021, 2:37 PM), https://www.forbes.com/sites/timbajarin/2021/04/29/work-from-home-is-the-new-normal-for-workers-around-the-world.

120. *See supra* text accompanying notes 26–36; *see also* U.S. CONST. amend. IV.

121. *See Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting) (noting the majority's multifactor analysis, which considers intimacy, comprehensiveness, expense, retrospectivity, and voluntariness). Police expense is left to one side because lower expenditures for investigations are not the kind of thing one thinks of when a government agency seeks to investigate. That is, there is no dollar amount to constitutional protections. Although some may argue that a reduction of police expenses leads toward unreasonable government searches, there is no compelling reason to predicate unreasonableness on a reduction of tax-payer costs.

122. *See id.* at 2220 (majority opinion).

123. *See id.* at 2234 (Kennedy, J., dissenting).

III. ZOOM'S PRIVACY POLICY – GOVERNMENT REQUESTS

A. *The Policy*

Zoom's privacy policy details exactly what the platform captures and stores, and provides a specific privacy policy for Government Requests.[124] The policy requires that the government submit requests in accordance with applicable laws and rules, subject to additional scrutiny for "certain" requests for data.[125] Data collected includes both data "provided" to Zoom and data that Zoom's system collects.[126] Additionally, Zoom will collect and maintain recorded meetings and chats to the extent that the meeting host opts-in for such functions.[127]

Zoom collects data provided by the user. Its government request guide states:

> Depending on whether or not a user has a registered Zoom account and which product or service is used, we may collect the following data from our users, which we may or may not retain depending on the type of data and our applicable retention policy:
>
> ***Identifying information***, including, name, username, email address, or phone number, as well as account owner name, billing name and address, and payment method (we do not store any user credit card information); for Zoom Phone users, the phone number dialed;

124. *See generally Government Requests Guide*, NAT'L SCI. FOUND., ZOOM, https://nsf.zoomgov.com/docs/en-us/government-requests-guide.html (last visited Jan. 12, 2022) [hereinafter *Zoom Government Requests*].

125. *Id.*

126. *Id.*

127. *Id.*

> ***Other account data***, including language preference, hashes of the password, title, department, profile photo; and
>
> ***User content*** that a user chooses to store to the Zoom cloud or provide to us, including cloud recordings, transcripts, chat and instant messages, files, whiteboards, voicemails for Zoom Phone users.[128]

Data that Zoom collects about users, products, and services includes the passively conveyed information included below. The relevant parts of the policy state:

> ***Technical information*** about a user's device, network, and internet connection, including the user's IP address, MAC address, other device ID (UDID), device type, how the user connected, network performance, operating system type and version, client version, type of camera, microphone, or speakers; for Zoom Phone users, the phone number of the user making the call;
>
> ***Approximate location*** to nearest city;
>
> ***Metadata***, including duration of the meeting or Zoom Phone call; email address, name, or other information that participants enter to identify themselves in a meeting, join and leave time of participants, meeting name, the scheduled date and time of a meeting, call data records for Zoom Phone.[129]

Notably, Zoom automatically captures meeting metadata and stores it in Zoom databases.[130] Even after a user deletes an account, there is a window of time in which Zoom can access

128. *Id.*
129. *Id.*
130. *Id.*

that account information and the corresponding data so long as it is stored in Zoom's cloud.[131]

Zoom's Government Request policy further states that it will release particular information compelled by a subpoena or court order, that is, without probable cause.[132] This information includes "user, account, and meeting data (not including contents of communications), which, if available, may include: name, email address, phone number, meeting metadata, IP address, MAC address, other device ID (UDID), and approximate location."[133] On the other hand, Zoom indicates that the government would need to provide a search warrant to compel disclosure of "users' stored content data, which may include cloud recordings, transcripts, chat/instant messages, files, whiteboards, and other information shared while using our services."[134]

However, in both these categories—release of information requiring a subpoena and information requiring a warrant—Zoom states that either document is "required to *compel* [] disclosure."[135] That is, the policy is silent on whether Zoom, of its own volition, will *voluntarily* and unilaterally offer information in either category at the mere request of the government.[136] Again, according to the third-party doctrine, Zoom may choose to share this information at any given point and the government, of course, would not need to issue a warrant to a specific user for access to that content, as the user does not retain an expectation of privacy to such information once it is conveyed to Zoom.[137] Thus, this policy makes clear that Zoom stores meeting data and may relinquish it if the developers see fit, regardless of whether police have a

131. *See id.*

132. *See id.*

133. *Id.*

134. *Id.*

135. *Id.* (emphasis added).

136. *See id.*

137. *See generally* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (discussing the "reduced expectation of privacy" with respect to information "knowingly shared with another"); *see also Zoom Privacy Statement*, *supra* note 12.

warrant.[138] Furthermore, additional questions lie outside the realm of Zoom servers as "[a] recording of the video can be stored locally on the hard drive of a [users'] laptop or secured on Zoom's cloud storage with a password that the host creates and could, perhaps, share with others."[139]

B. *Zoom's Privacy Commitments*

Zoom has already agreed to work with law enforcement to track improper use of its platform.[140] Furthermore, case law interpreting exceptions to the third-party doctrine surrounding media platforms is split in lower courts.[141] The public should know whether the Fourth Amendment protects them from searches of data gathered by Zoom and similar platforms.

In a recent statement, Zoom announced its willingness to work with the FBI.[142] Zoom's CEO, Eric Yuan, stated in a call that Zoom plans to move ahead to disclose meeting information for those who use Zoom "for a bad purpose."[143] Zoom announced that these practices and willingness to work with the FBI were implemented to secure the platform from the exploitation of children, which any moral person would not argue against.[144] However, one potential concern is that there is "a history of the government using [the exploitation of children]

138. *See Zoom Privacy Statement*, *supra* note 12; *see also Zoom Government Requests*, *supra* note 124 (noting that some types of data, for example usernames or meeting metadata, can be released to authorities with only subpoenas and does not require a search warrant).

139. *See* Allen St. John, *Zoom Calls Aren't as Private as You May Think. Here's What You Should Know*, CONSUMER REPS., https://www.consumerreports.org/video-conferencing-services/zoom-teleconferencing-privacy-concerns/ (Mar. 30, 2020).

140. *See* Sara Morrison, *Zoom Wants To "Work Together" with the FBI. That May Not Be as Bad as it Sounds.*, VOX (June 3, 2020, 2:45 PM), https://www.vox.com/recode/2020/6/3/21279285/zoom-fbi-encryption-calls-free-users.

141. *See infra* Part IV.

142. Adi Robertson, *Zoom Says Free Users Won't Get End-to-End Encryption so FBI and Police Can Access Calls,* VERGE (June 3, 2020, 2:31 PM), https://www.theverge.com/2020/6/3/21279355/zoom-end-encryption-calls-fbi-police-free-users.

143. *See* Nico Grant, *Zoom Transforms Hype into Huge Jump in Sales, Customers*, BLOOMBERG (June 3, 2020, 11:52 AM), https://www.bloomberg.com/news/articles/2020-06-02/zoom-transforms-hype-into-huge-jump-in-sales-customers.

144. *See* Morrison, *supra* note 140.

crime to weaken [other] legal protections that affect everyone."[145] The question remaining is whether police investigations will require a warrant to access user data from Zoom.

Wherever Zoom lands with its decisions to work with the FBI moving forward, one thing is certain—although Zoom does encrypt both its free and paid calls, it only offers end-to-end encryption of its meetings in a limited and impractical context.[146] "Encryption is not the same as end-to-end encryption, which encrypts the message to everyone except the sender and receive. In other words, with end-to-end encryption, neither Zoom nor law enforcement would have a way to intercept and interpret messages."[147]

Put simply, "[w]hen a message is protected by end-to-end encryption, only the sender and recipient are able to read it."[148] This means that "[n]o matter how many servers or networks the message passes through on its way, it remains unreadable to anyone but the eventual recipient."[149] Notably, "[t]he impossibility of deciphering an encrypted message without a private key has raised concerns with law enforcement officials and politicians . . . ."[150]

Instead of utilizing such end-to-end encryption in all or most contexts, Zoom uses "256-bit AES-GCM" encryption as its default.[151] With this default encryption, "Zoom is not end-to-

145. *Id.*

146. *See id.*; *End-to-End (E2EE) Encryption for Meetings*, ZOOM HELP CTR., https://support.zoom.us/hc/en-us/articles/360048660871 (Dec. 15, 2021). The end-to-end encryption feature disables many features that make Zoom useful, including cloud recordings, chat transcripts, private chats, etc. *Id.* Additionally, the new statement on end-to-end comes after multiple years of involuntary use expressed in this Note. *See id.* Questions regarding whether the platform will allow end-to-end encryption to be retroactively applied to meeting data already stored on its servers are not addressed. *See id.*

147. Morrison, *supra* note 140.

148. *Client-Side Encryption vs. End-to-End Encryption: What's the Difference?*, PKWARE: BLOG (Feb. 28, 2017),
https://www.pkware.com/blog/client-side-encryption-vs-end-to-end-encryption-whats-the-difference.

149. *Id.*

150. *Id.*

151. Max Krohn, *Zoom Rolling Out End-to-End Encryption Offering*, ZOOM BLOG,

end encrypted, [and] even if meetings remain encrypted on their whole route across the internet, . . . Zoom *could* use the keys it holds to decrypt the data during that journey."[152] That is, Zoom "'[s]aying they don't decrypt [the data] at any point does not mean that they *cannot* decrypt it at any point,' says Brown University cryptographer Seny Kamara."[153]

At any rate, Zoom recently released end-to-end encryption capabilities for its service "but will only offer them to business and enterprise customers whose identities the company can confirm."[154] Zoom further stated that once end-to-end encryption does become available to their users, it plans "to provide [it] to users for whom we can verify identity, thereby limiting harm to these vulnerable groups . . . . Free users sign up with an email address, which does not provide enough information to verify identity."[155] Zoom stated that this limitation exists to enable law enforcement to investigate crimes.[156] The question of whether this essential service is protected by the Fourth Amendment broadens in light of its questionable encryption methods.

C. *Family Educational Rights and Privacy Act*

Under the Family Educational Rights and Privacy Act (FERPA), universities are generally required to get student permission to disclose personally identifiable information (PII) and records gathered about the student.[157] However, FERPA's regulations explicitly authorize disclosure by an agency or institution to comply with a lawfully issued subpoena.[158] This

https://blog.zoom.us/zoom-rolling-out-end-to-end-encryption-offering (Aug. 3, 2021); *End-to-End (E2EE) Encryption for Meetings*, *supra* note 146.

152. Lily Hay Newman, *So Wait, How Encrypted Are Zoom Meetings Really?*, WIRED (Apr. 3, 2020, 12:44 PM), wired.com/story/zoom-security-encryption/; *see also End-to-End (E2EE) Encryption for Meetings*, *supra* note 146.

153. Newman, *supra* note 153 (emphasis added).

154. *See* Morrison, *supra* note 140.

155. *Id.*

156. *See id.*

157. *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

158. § 1232g(b)(2)(B); 34 C.F.R. § 99.31(a)(9)(i) (2021).

means that, although universities usually must get student consent to disclose information, pursuant to FERPA, such protections do not transcend a subpoena.[159]

The Act defines "education records" as any "records, files, documents, and other materials which . . . (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution."[160] And, coincidentally, the regulation defining terms within FERPA defines "record" to mean "*any information recorded in any way, including*, but not limited to, handwriting, print, *computer media, video or audio tape*, film, microfilm, and microfiche."[161] Moreover, "[i]t is important to note that any of these records maintained by a third party acting on behalf of a school or district are also considered education records."[162]

Presumably schools have Zoom data available, i.e., class recording and chats, and would otherwise need consent under FERPA to disclose such data to the extent it relates to particular student, but when Zoom "owns" the material, how does this brush up against FERPA and its consent requirements? Is Zoom, as a private entity, required to comply with the FERPA standard even though it technically becomes the "owner" of data held within its servers? Thankfully, the U.S. Department of Education's Privacy Technical Assistance Center has made clear that Zoom must comply with FERPA.[163] Zoom has since issued a guide outlining its effort to maintain compliance with the Act.[164] However, Zoom's good faith compliance may be open to interpretation during these changing times. As Zoom stated in its FERPA Guide, although it plans to comply with

159. *See* § 1232g(b)(2)(B).

160. § 1232g(a)(4)(A)(i)–(ii).

161. 34 C.F.R. § 99.3 (2021) (emphasis added).

162. U.S. DEP'T OF EDUC. PRIV. TECH. ASSISTANCE CTR., RESPONSIBILITIES OF THIRD-PARTY SERVICE PROVIDERS UNDER FERPA 1 (2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor20FAQ.pdf.

163. *See id.* at 2.

164. *See* FERPA GUIDE 2, ZOOM (Oct. 2020), https://explore.zoom.us/docs/doc/FERPA%20Guide.pdf [hereinafter ZOOM FERPA GUIDE].

FERPA, it "collects and uses student PII that it needs to provide and improve our services or as otherwise directed by the School Subscriber."[165]

At any rate, students are at best protected by the subpoena requirement,[166] but subpoenas, unlike warrants, do not require probable cause and do not implicate Fourth Amendment protection.[167] So, even though student information must pass through one additional hoop for the government to gain access, such data is still subject to lesser protection than if a warrant were required.[168] Taking the nontraditional data—e.g., retrospective views into the students' homes, locations during meetings, etc.—collected by Zoom[169] out of the hands of the student and placing it into the hands of respective educational institutions and Zoom, where it is protected only minimally by the subpoena requirement, should implicate an unreasonable search under the Fourth Amendment.[170] The data shared by a student over Zoom extends far beyond what one would consider to be the traditional "records" maintained by institutions. Moreover, such conveyance of data is not voluntary, because the student must join the Zoom classroom, or otherwise choose to forego any meaningful education during or after the pandemic to the extent the institution retains online options.[171] Thus, this nontraditional data collected by schools

165. *See id.*

166. *See* 34 C.F.R. § 99.31(a)(9); 20 U.S.C. § 1232g(b)(I)(J), (b)(2)(B).

167. *See supra* note 48.

168. *Id.*

169. *See* ZOOM FERPA GUIDE, *supra* note 165 (discussing traditional educational records); Richie Koch, *Using Zoom? Here Are the Privacy Issues You Need to Be Aware of*, PROTONMAIL (Mar. 20, 2020), https://protonmail.com/blog/zoom-privacy-issues/ (discussing the data Zoom collects).

170. *See supra* text accompanying note 165; *see generally* 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 . . . .").

171. *See infra* Section IV.B.

and Zoom should fall within the purview of a search and should require a warrant for access.[172]

D. *Employee Rights to Privacy*

As previously discussed, the Court in *Carpenter* issued its holding with respect to the Stored Communications Act on narrow grounds—applying the holding to as little as seven days' worth of CSLI data.[173] However, as this Note suggests, there are additional and novel considerations regarding privacy moving forward—mainly the camera lens broadcasting a recording inside the employee's home. Employees are similarly situated to students, as the Stored Communications Act allows the Government to compel the release of electronic communication data through a court order, or subpoena, so long as the Government provides "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[174] As outlined earlier, this standard likewise does not require probable cause and is thus lower than the standard of a warrant.[175]

Additionally, employees may be at a further disadvantage when it comes to Zoom. The Electronic Communications Privacy Act of 1986 allows employers to intercept and monitor employees' electronic communications so long as the employer is *providing* the communication service.[176] And, of course, once the employer entrusts data to a third party, the data falls subject

172. *See generally supra* notes 14–25 and accompanying text and note 48 (discussing the standard for a Fourth Amendment search and the requirements for issuance of a warrant).

173. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213, 2220 (2018).

174. Stored Communications Act, 18 U.S.C. § 2703(d). The previous section of the Act does place limitations on electronic communication providers from knowingly divulging information, however, governmental access remains available via subpoena. *See id.* § 2702.

175. *See supra* text accompanying notes 14–36, 132–39.

176. *See* Stored Communications Act, § 2701(c). The Act broadly states that it is illegal to intercept electronic communications but explains that an exception exists for an "entity providing [an] electronic communication service." *Id.*

to the third-party doctrine.[177] There may be room for debate regarding the tensions between employer and employee when it comes to the ownership and privacy rights implicated by stored videoconferencing data. Because employees are generally considered agents of their employers,[178] this Note presupposes that the employer maintains ownership rights to data collected in the course of employment.[179] However, in *Carpenter*, the fact that the individual did not *own* the information shared with a third party "[did] not negate [the individual's] anticipation of privacy."[180]

Just like students, the use of Zoom by employees involves the collection of nontraditional electronic data between employer and employee, subject to the control of Zoom—the third party.[181] This data is so far removed from traditional employment endeavors that the Fourth Amendment must step in.[182] According to the Stored Communications Act, the government may compel employers and Zoom to release data just as easily as the FERPA standard conveys; that is, through court order.[183] Thus, while the Zoom privacy policy states that it requires a warrant to *compel* the of release stored communications in its cloud,[184] the Stored Communications Act clearly states otherwise; and surely a federal statute preempts a

177. *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (discussing how information loses Fourth Amendment protection under the third-party doctrine when that information is knowingly revealed to a third party).

178. *See Respondeat Superior*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/respondeat_superior (last visited Jan. 1, 2022).

179. *See* discussion *supra* Part II.

180. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

181. *See Zoom Privacy Statement*, *supra* note 12 (listing the various types of information Zoom may collect); ZOOM FERPA GUIDE, *supra* note 165 (mentioning that, among other records relating to students' personal data, "[v]ideo recordings/streams, chat logs, [and] transcripts" are available for schools to collect from Zoom).

182. *See Zoom Privacy Statement*, *supra* note 12; Karin Kashi, *Collecting Employee Information? It's Time to Wake Up*, JD SUPRA (Jan. 12, 2021), https://www.jdsupra.com/legalnews/collecting-employee-information-it-s-6974458/ (noting that employers typically collect employee data like salary information, resumes, work hours, medical information, messages on company devices, and location data on company vehicles).

183. *See* Stored Communications Act, 18 U.S.C. § 2703(d); 20 U.S.C. § 1232g(b)(2)(B).

184. *See Zoom Government Requests*, *supra* note 124.

company policy.[185] In conclusion, given the parameters of the third-party doctrine and the statutes regulating academia and employment, both students and employees are left protected only by the thin veneer of a subpoena.

IV. APPLYING *CARPENTER* TO ZOOM IN LIGHT OF LOWER COURTS OPINIONS

With the foregoing backdrop in place, the question remains as to how lower courts are handling the Fourth Amendment doctrine in light of *Carpenter*. It is unclear whether Zoom privacy maps on to *Carpenter*'s holding, given how different courts have interpreted this holding. Courts have already begun to struggle with how to apply the *Carpenter* Court's interpretation of what constitutes a reasonable expectation of privacy regarding third-party technology, with some deciding against defendants' rights to privacy and others supporting privacy rights.[186]

However, one court offered a glimpse of hope concerning the scope of *Carpenter*. The court in *United States v. Kidd* raised questions regarding just how far *Carpenter* extends.[187] The court ascertained whether use of IP address information gathered by Pinger, a telecommunications provider, fit under *Carpenter*, while rejecting the bright-line rule in other cases that asserted IP address information squarely fell outside the purview of *Carpenter*.[188] The court noted that "[e]xtending *Carpenter* to new areas requires a precise understanding of the technology at issue, as demonstrated by the discussion of technology in *Carpenter* itself."[189] The court asserted that in determining whether information gathered by police through a third party is sufficiently analogous to *Carpenter* depends on a fact-intensive analysis including inquiry into (1) whether the

185. *See* Stored Communications Act § 2703(d).

186. *See* cases discussed *infra* Section IV.A.

187. *See* United States v. Kidd, 394 F. Supp. 3d 357, 364–65 (S.D.N.Y. 2019).

188. *Id.* at 362, 364–65.

189. *Id.* at 367.

application gathered information when the user was not actively using the platform; (2) whether the platform was capable of being used outside the house through a cellular network; and (3) how geographically precise the information resulting from the data collected is.[190]

Kidd's willingness to reconcile the technology at hand with *Carpenter*'s fact-intensive analysis, as opposed to adopting the bright-line holding as other courts have, offers an optimistic beacon in an otherwise chaotic assembly of third-party doctrine precedent; some courts may be willing to limit the broad boundaries of the doctrine. At any rate, to understand why Zoom data regulation should likewise fit outside the scope of the third-party doctrine, an exploration into the relevant factors—comprehensiveness, voluntariness, intimacy, and retrospectivity—discussed in *Carpenter* is in order.[191]

A. *Comprehensiveness*

A cellphone is not the only machine capable of comprehensively storing and providing data about its users to third parties. As outlined above, Zoom's privacy policy is a case in point.[192] That is, the videoconferencing platform expressly states exactly what information it stores on behalf of any and all of its users, including and extending beyond location information.[193] Problems concerning comprehensiveness have already begun to arise following the *Carpenter* holding. For example, the court in *In re Google Location History Litigation* cut against privacy expectations, stating that location information collected and stored by Google media applications fell outside the purview of *Carpenter* because "not *all* of Plaintiff's movements were being collected, *only specific movements or*

190. *Id.* at 367–68.

191. *See* Carpenter v. United States, 138 S. Ct. 2206, 2234 (2018).

192. *See supra* Section III.B.

193. *See Zoom Privacy Statement*, *supra* note 12.

locations."[194] The court elaborated that *Carpenter*'s holding instead addressed cellphones comprehensively tracking "nearly exactly" where a person goes.[195] Thus, "[s]uch 'bits and pieces' [did] not meet the standard of privacy established in *Carpenter*."[196]

On the other hand, in *Commonwealth v. Almonor*, the Massachusetts Supreme Court held in favor of a defendant's reasonable expectation of privacy to his singular, real-time location accessed through his cellphone provider.[197] There, a murder suspect was found at his home after police contacted his cell company to ping his current location, which allowed the police to access only a *single location*, which led to the defendant's arrest.[198] The court stated that "society reasonably expects that the police will not be able to secretly manipulate our personal cellphones for any purpose, let alone for the purpose of transmitting our personal location data."[199]

These two cases present the very problem that arose from *Carpenter*'s narrow holding. *Google* says, "bits and pieces," and not *all*, of exact locations were insufficient to map on to *Carpenter*,[200] while *Almonor* simply says one location is sufficient to bring the case under *Carpenter*'s protection.[201] *Carpenter* could have resolved this tension in the lower courts had it held that comprehensiveness of searches involves, for example, specificity in the location of the user. Zoom and the data it collects offers a comprehensive chronology of its user's access by capturing and storing a myriad of identifiable information in Zoom databases.[202] Given how pervasive the use of Zoom is today and its likelihood to maintain, this comprehensive script

194. *In re* Google Location Hist. Litig., 428 F. Supp. 3d 185, 198 (N.D. Cal. 2019) (emphasis added).

195. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2218).

196. *Id.*

197. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1193 (Mass. 2019).

198. *Id.* at 1186–87.

199. *Id.* at 1193–94.

200. *See In re Google*, 428 F. Supp. 3d at 198.

201. *See Almonor*, 120 N.E.3d at 1202 (Lenk, J. concurring).

202. *See Zoom Privacy Statement*, *supra* note 12.

of user data gives the government access to a broad array of information about people that would otherwise be unavailable.[203] As such, Zoom should fit within the comprehensiveness factor discussed in *Carpenter*.

A proponent of the third-party doctrine may contend that *Carpenter* is still distinguishable from the issues presented with Zoom and its privacy policy. Zoom, unlike the cellphone in *Carpenter*, is not active at all times, nor is it actively storing data merely by the passive powering on of a device.[204] As such, *Carpenter*'s use of 12,898 individual locations spanning 127 days[205] is a far cry from the less frequent use of Zoom or any other videoconferencing platform for that matter. In this way, Zoom is more like the "bits and pieces" of data collected in *Google*, which were insufficient to establish and maintain a person's reasonable expectation of privacy.[206] Thus, the government—seeking to preserve the doctrine—may argue that the "some but not all" rationale that supported the lack of privacy expectation in *Google* should likewise apply in the case of Zoom.[207] That is, unlike *Google*'s application, cellphones are significantly more pervasive because they track people "nearly exactly."[208] Moreover, a proponent of the third-party doctrine could argue against a reasonable expectation of privacy to the data collected by Zoom, asserting that like in *Almonor*, only real time access to location should trigger *Carpenter*.[209] This argument suggests that real-time access of locations should be the controlling rationale to maintain a reasonable expectation of privacy.

The opinions in *Almonor* and *Google* cannot fairly align with *Carpenter* if the concern is really the determination of "exact

203. *See id.*; Iqbal, *supra* note 11.
204. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
205. *See id.*
206. *See In re* Google Location Hist. Litig., 428 F. Supp. 3d 185, 198 (N.D. Cal. 2019).
207. *See id.*
208. *See id.*; *see also Carpenter*, 138 S. Ct. at 2218.
209. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1194 (Mass. 2019).

location."[210] First, *Carpenter* held that the public retains a reasonable expectation of privacy with respect to as little as seven days of CSLI data.[211] And, quite simply, Carpenter asserted that the fifty-meter radius triangulation of involuntarily shared data was subject to Fourth Amendment protection.[212] Thus, although *Carpenter* did use the language "nearly exactly,"[213] factual context suggests the Court's use of the word "nearly" fell within a radius of a half mile to two miles in all directions. The language is ambiguous at best, but the courts in *Almonor* and *Google* certainly misread the text, allowing for a misguided, less charitable approach to the word "nearly" than *Carpenter* did.[214]

As *Kidd* properly notes, courts ought to examine three factors: (1) the extent to which the application or platform actively gathered information when not in use, (2) whether it may be used outside the home on a cell network, and (3) how geographically accurate the location information was.[215] As mentioned above, a closer look at *Google* reveals the court was incorrect to conflate its precise locations with *Carpenter* and its cellphone tracking that provided *nearly exact* location information.[216] That is, the police in *Carpenter* relied on a radius of the defendant's location via CSLI to place him at or near crimes committed; thus, the standard in *Carpenter* is not pin-pointed exactness but an ability to generate a radius indicating a person's exact location.[217]

Applying the *Kidd* test demonstrates: (1) Zoom operates on both cell networks and internet service provider networks, which constitutes sufficient use outside the home and (2) just like the use of triangulation, Zoom can access similar cellphone

210. *See Carpenter*, 138 S. Ct. at 2219; *Almonor*, 120 N.E.3d at 1193; *In re Google*, 428 F. Supp. 3d at 198.

211. *See Carpenter*, 138 S. Ct. at 2217, n. 3.

212. *See id.* at 2219–20.

213. *See id.* at 2218–19.

214. *See id.* at 2218; *Almonor*, 120 N.E.3d at 1193; *In re Google*, 428 F. Supp. 3d at 199.

215. United States v. Kidd, 394 F. Supp. 3d 357, 367–68 (S.D.N.Y. 2019).

216. *See In re Google*, 428 F. Supp. 3d at 198.

217. *See Carpenter*, 138 S. Ct. at 2219.

provider networks that supported an expectation of privacy in *Carpenter*.[218] Finally, Zoom is accessible through Windows and iOS operating systems, all smartphone devices, and all tablets and laptops.[219] These devices are readily available to function both outside the home and on a cell network.[220] Zoom also collects and stores data including recordings, chats, transcripts, audio files, etc.—which plainly and categorically exceeds the already "comprehensive" location data collected in *Carpenter*, thereby implicating an aggregation of new search features available to the government.[221] Thus, Zoom should fall within the comprehensiveness rationale in *Carpenter* used to support a reasonable expectation of privacy.[222] Specifically, recorded videos, chats, time-stamped entries into virtual spaces, and location data accessible through the Zoom cloud certainly ought to map onto—and exceed—the comprehensiveness discussed in *Carpenter*.[223]

B. *Voluntariness*

Put simply, members of society are not actively choosing to use videoconferencing as their primary mode of communication. Post-pandemic use of videoconferencing will likewise not extend into the voluntary sharing of information that motivated both *Smith* and *Miller*.[224] People are *required* to adapt to how employers and schools—as opposed to an autonomous individual—choose to continue utilizing videoconferencing.[225] This adaptation on account of the

218. *See Kidd*, 394 F. Supp. 3d at 368; *see also* Mitja Rutnik, *How to Set Up and Use Zoom: Everything You Need to Know to Get Started*, ANDROID AUTH. (June 6, 2021), https://www.androidauthority.com/how-to-use-zoom-meetings-1100614/ (explaining how to use Zoom without an internet connection via Zoom's mobile app).

219. *See* Rutnik, *supra* note 221.

220. *See id.*

221. *See Carpenter*, 138 S. Ct. at 2217; *Zoom Privacy Statement*, *supra* note 12.

222. *See Carpenter*, 138 S. Ct. at 2232.

223. *Id.*

224. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

225. *See, e.g.*, Superville, *supra* note 1 (stating that, in a survey of school administrators,

individual is not analogous to *Smith* or *Miller* because no entity in either case *compelled* the defendants to engage in the use of bank notes or pen registries.[226] Instead, students and employees alike are prodded by their respective institutions to engage in these interactions.[227] As a result, data attached to each student and employee using Zoom that in-person interactions would simply not otherwise yield, now floats in the ether, owned by parties outside of the individual's formal, voluntary control.

Another case worth exploring, *United States v. Hood*, proved problematic for the application of voluntariness that *Carpenter* and the Fourth Amendment seek to protect. In *Hood*, the First Circuit held that *Carpenter* did not apply to subscriber information revealed by a messaging service provider in response to an Emergency Disclosure Request from the government.[228] The information was available to the government through the third-party doctrine.[229] The information collected included data that revealed the user's IP address, date and time of service, a user email address, and the type of device used to access the account.[230] The court reasoned that an IP address, unlike CSLI in *Carpenter*, was not subject to an expectation of privacy because (1) it did not itself reveal any location information, and (2) there were active steps in generating IP address information, which were considered voluntary, while CSLI was passively generated.[231] However, the information gathered was then, in turn, used to enable police to determine both the exact location of the user when he logged in

20% said they were planning on being fully remote in the upcoming academic year).

226. *See Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 442.

227. As early as April 2020, 90,000 schools had switched to Zoom as their educational platform, and at least 58,496 companies were also using Zoom. Mark Lieberman, *Zoom Use Skyrockets During Coronavirus Pandemic, Prompting Wave of Problems for Schools*, EDUC. WEEK (Apr. 6, 2020), https://www.edweek.org/technology/zoom-use-skyrockets-during-coronavirus-pandemic-prompting-wave-of-problems-for-schools/2020/04; *Companies Using Zoom*, ENLYFT, https://enlyft.com/tech/products/zoom (last visited Jan. 13, 2022).

228. United States v. Hood, 920 F.3d 87, 91–92 (1st Cir. 2019).

229. *Id.* at 91.

230. *Id.* at 89.

231. *Id.* at 92.

to the messaging platform and the date and time of the transmissions.[232] Most importantly, the *Hood* court emphasized that, "an internet user generates the IP address data . . . only by making the *affirmative decision* to access a website or application."[233]

In the context of Zoom, a proponent of the third-party doctrine could argue that *Hood* got it right. Particularly, data produced as a product of videoconferencing platforms is likewise only available after the user makes the affirmative decision to access the application.[234] The proponent of the third-party doctrine could also assert that Zoom is wholly distinguishable from *Carpenter*, as the reasoning in *Carpenter* flowed from the fact that a cellphone produces CLSI merely as a product of simply powering the phone on, whereas a Zoom user must power on a device and then subsequently access the app and log-in before the app produces any data.[235]

However, this argument presupposes a level of free will and agency that is just not available in society's current endeavors. The argument supporting the third-party doctrine operates within a two-dimensional framework that includes *only* (1) the individual and (2) the respective device collecting information. And, so far, the analysis hinges on the individual's active or passive agency relating to the production of data. For instance, the third-party doctrine renders the active decision to access a website or application unprotected by the Fourth Amendment, while the passive decision—or lack of any formal, voluntary effort—motivates Fourth Amendment protection under *Carpenter*.[236]

232. *Id.* at 91.

233. *Id.* at 92 (emphasis added). The court did not address the government's ability to extract location information but noted that other courts have also held that IP address information is not protectable under the Fourth Amendment. *Id.*; *see, e.g.*, United States v. Morel, 922 F.3d 1, 9 (1st Cir. 2019) (upholding warrantless search of IP address information).

234. *See Hood*, 920 F.3d at 92.

235. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018); Rutnik, *supra* note 221.

236. *See Carpenter*, 138 S. Ct. at 2220.

In the context of employees and students using Zoom, this two-dimensional framework simply does not fit because there is an additional agent embedded in the employee's or student's decision to access Zoom—their respective institutions. This third party removes the individual's complete volition and voluntary action and, in a sense, guides the user's actions to access the videoconferencing platform, thus stripping the student and the employee of the affirmative decision that minimizes their Fourth Amendment protections.[237] Put simply, this reality cuts against free agency, affirmative decisions, and voluntary use.[238]

Although Zoom issued a statement explaining its compliance with FERPA's guidelines,[239] academic institutions hold a concerning amount of student data conveyed involuntarily through Zoom. Should a student have to consent via FERPA to the release of information stored through Zoom? Class recordings peering into the home of each student instructed to turn their camera on during class *should* implicate a reasonable expectation of privacy and should, therefore, require a warrant. A recording into one's home is vastly different from a transcript or other academic document traditionally protected by FERPA; however, the language of the FERPA regulation now states that a school will turn over a student's information when supported by subpoena or court order.[240] This provision seems to involve an unforeseeable oversight in the regulation's language, given the novel and delicate nature of the data collected today.

Similarly, employers' use of Zoom as a mode of employment communication also requires employees to convey data in ways not traditionally collected or considered to be voluntary. Like academia, traditional employee communications such as email

237. *See id.*

238. *See generally* Manyu Jiang, *The Reason Zoom Calls Drain Your Energy*, BBC: REMOTE CONTROL (Apr. 22, 2020), https://www.bbc.com/worklife/article/20200421-why-zoom-video-chats-are-so-exhausting (theorizing the reasons for Zoom fatigue and ways Zoom users can alleviate those symptoms).

239. *See* ZOOM FERPA GUIDE, *supra* note 165.

240. *See* 34 C.F.R. § 99.31(a)(9)(i) (2021).

or telephone records are vastly different from the novel data collected by Zoom.[241] Again, recordings into one's home transcends what ought to be covered by the Stored Communications Act and should require a warrant, not just a mere subpoena or court order.[242] Again, *Carpenter* supported protection under the Fourth Amendment because a cellphone "faithfully follows its owner beyond public thoroughfares and into private residences" and the same reasoning should apply to Zoom.[243]

At any rate, despite the interpretation of *Carpenter* under *Hood*,[244] an institution's choice to mandate the exclusive use of one videoconferencing platform, such as Zoom, for its employees or students is a significant departure from any sort of recreational use of videoconferencing.[245] Essentially, society is faced with a genuine option of either (1) using the videoconferencing platform of the institution's choice or (2) foregoing any meaningful education or employment opportunity.[246] Thus, Zoom use in the employment and education contexts falls outside the scope of any traditionally understood meaning of voluntary use and should not be subject to the third-party doctrine.

241. *See Zoom Privacy Statement*, *supra* note 12.

242. *See* Stored Communications Act, 18 U.S.C. § 2703(d).

243. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

244. *See* United States v. Hood, 920 F.3d 87, 91–92 (1st Cir. 2019).

245. *See* Dan Sinker, *The Crushing Reality of Zoom School*, ESQUIRE (Sept. 16, 2020), https://www.esquire.com/news-politics/a34028673/parenting-pandemic-zoom-school/ (describing the difficulties the author and his family experienced using Zoom for work and school).

246. This is an inference drawn given the circumstances of the virtual setting that was present at the time this Note was written. *See, e.g.*, Ellie Silverman, *Some Colleges Welcome Students Back, Others Move All-Online*, PHILA. INQUIRER (Aug. 19, 2020), https://www.inquirer.com/health/coronavirus/newsletter/covid19-coronavirus-temple-pennsylvania-state-drexel-universities-college-campus-online-20200819.html ("Drexel University's president announced today that the Philadelphia school will have online-only undergraduate classes for the fall quarter.").

C. *Intimacy*

Although *Carpenter* was correct in its characterization of the government's pervasive and warrantless tracking, such a degree of intrusion is not even necessary to call into question whether someone retains an expectation of privacy.[247] Other courts have refused to extend the rule regarding data collected by third parties to circumvent the third-party doctrine under *Carpenter*, often relying on the fact that IP information is generated inside the home, which, unlike *Carpenter*, does not 'follow' the user to such a pervasive extent.[248] However, the Fourth Amendment was initially adopted to circumvent government intrusions *into* the home.[249] Thus, even to the extent that a person uses Zoom strictly from their home, exposures to the interior of the home should be subject to an expectation of privacy that society is willing to recognize.[250] The Court in *Kyllo v. United States* plainly supported this proposition when it asserted that use of technology to gather any information "to explore details of the home that would previously have been unknowable without physical intrusion" constitutes a search and requires a warrant.[251]

Courts should take notice that Zoom is available for use on nearly every smart device and is thus analogous to the intimacy reasoning supporting *Carpenter*.[252] However, when accepting

247. *See Carpenter*, 138 S. Ct. at 2217–18.

248. *See* United States v. Tolbert, No. 14–3761, 2019 WL 2006464, at *3 (D.N.M. May 7, 2019); United States v. McCutchin, No. CR-17-01517-001, 2019 WL 1075544, at *3 (D. Ariz. Mar. 7, 2019); United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018).

249. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

250. *See id.*

251. *Id.* at 40. Though the *Kyllo* decision hinged on technology not available to the general public, the decision is clearly applicable to technology generally available today. That is, Justice Scalia's majority expressed concern for searches that "would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home"—a concern that videoconferencing platforms provoke. *Id.* at 35–36.

252. *See Carpenter*, 138 S. Ct. at 2217–18 (reasoning that time-stamped cellphone location data "provides an intimate window into a person's life" and reveals far more about someone than

the involuntary use of Zoom, utilizing the platform is even more intimately pervasive than the reasoning that supported *Carpenter*.[253] Data collected by Zoom not only tracks a person's locations when connected to a cellular data network, but also opens a lens into our most private sphere.[254] Thus, Zoom functions more intimately in the home than CSLI; while CSLI merely indicates presence in an area, the Zoom privacy policy indicated a much higher degree of intimate detail collected, including login and logout times, schedules, meeting recordings, transcripts, and who we associate with over the application.[255] In essence, Zoom not only follows the user into the home, but it opens an eye into the home and gives the government an on-demand compilation of domestic episodes, which surely implicates a reasonable expectation of privacy—unless, of course, a party welcomes such intrusion.[256]

D. *Retrospectivity*

The last factor analyzed in *Carpenter* was the government's ability to seamlessly look back in time to track a defendant's movements.[257] Again, the Court expressed concern that the "[g]overnment can now travel back in time to retrace" data attached to each individual that would be "otherwise unknowable," "subject only to the retention polices of the wireless carriers."[258] At first glance, this concern should be the easy argument. *Carpenter* was concerned that retrospective access to CSLI did not require police to know who they wanted

just his or her "particular movements," since cellphones accompany their owners "beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales"); *see, e.g.*, Jeff Smith, *Zoom Expands to Smart Displays at Home*, ZOOM: BLOG (Aug. 19. 2020), https://blog.zoom.us/zoom-expands-to-smart-displays-at-home.

253. *See supra* Section I.B.

254. *See supra* Part II; *Zoom Privacy Statement*, *supra* note 12.

255. *See Zoom Privacy Statement*, *supra* note 12.

256. *See supra* Section III.A (discussing ways in which government can compel Zoom to turn over user data).

257. *Carpenter*, 138 S. Ct. at 2217–18.

258. *Id.* at 2218.

to target prospectively, and Zoom presents the same issues concerning its users' stored data.[259]

However, the application of this concern and type of data it attaches to has again been subject to ambiguity. In *United States v. Hall*, the court held that the defendant was not free from the doctrine despite being implicated for money laundering *after* police accessed his location through use of his bank card.[260] The defendant in *Hall* argued that he was not voluntarily sharing his location in a formal sense when using his bank card; therefore, police access of his *past* transactions should be subject to a legitimate expectation of privacy, just as CSLI was in *Carpenter*.[261] The court left the question of voluntariness aside but did respond to the retrospective nature of the search.[262] Even though police investigators were able to pinpoint his precise location retrospectively, the *Hall* court merely relied on the fact that *Carpenter* was a "narrow" holding pertaining to CSLI and ultimately dismissed the defendant's argument.[263]

Hall demonstrates that courts have had a tough time pinpointing what exactly to focus on following *Carpenter*, just as Justice Kennedy predicted.[264] Although the *Hall* court's reasoning would more than likely simply map on to the pen register record held subject to the third-party doctrine in *Smith*, the takeaway from *Hall* is that ambiguity exists surrounding the Fourth Amendment doctrine's application to advancing technology that is retrospectively available to the government.[265] The court in *Hall* was probably correct to deny the defendant's motion to suppress, as a reasonable expectation of privacy should not be maintained for bank card use, just as

259. *See id.*

260. *See* United States v. Hall, No. 16-CR-050-01, 2019 WL 5892776, at *5 (M.D. Pa. Nov. 12, 2019).

261. *Id.* at *5.

262. *See id.*

263. *Id.*

264. *See Carpenter*, 138 S. Ct. 2234 (Kennedy, J., dissenting).

265. *See Hall*, 2019 WL 5892776, at *5; *see also* Smith v. Maryland, 442 U.S. 735, 742–43 (1979).

the *Carpenter* Court reaffirmed.[266] However, the court in *Hall* only broadly covered what *Carpenter* decided, without ever taking into consideration exactly what should be controlling in analogous situations.[267] As such, the question still remains—is *Carpenter* dictated by its narrow holding? The retrospectivity factor was apparently insufficient to maintain a reasonable expectation of privacy in *Hall*, but the court, as Justice Kennedy warned, was quick to dismiss the defendant's argument without analyzing the other relevant factors discussed in *Carpenter*.[268]

As far as the data collected by Zoom goes, an abundance of information that would similarly be unknowable now sits statically in the Zoom cloud available for retrospective access.[269] And, just like the *Carpenter* Court expressed, this abundance of data is likewise subject to the retention policies of Zoom.[270] Although *Hall* relied on the literal interpretation of Chief Justice Roberts' holding to dismiss the defendant's argument,[271] such a limited reading of the language of *Carpenter* is not only myopic, but imprudent. Zoom should be the easy answer to Fourth Amendment protections extending to data collected by a third-party in light of *Carpenter*; however, until lower courts have clear guidance, ambiguity regarding Fourth Amendment doctrine persists.[272] Not only does Zoom collect information regarding location information,[273] but it likewise stores login

266. *See Hall*, 2019 WL 5892776, at *5; *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting) ("According to today's majority opinion, the Government can acquire a record of every credit card purchase . . . a person makes over months or years without upsetting a legitimate expectation of privacy.").

267. *See Hall*, 2019 WL 5892776, at *5; *Carpenter*, 138 S. Ct. at 2222.

268. *See Hall*, 2019 WL 5892776, at *5; *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting).

269. *See Zoom Privacy Statement*, *supra* note 12.

270. *Carpenter*, 138 S. Ct. at 2218; *see Zoom Privacy Statement*, *supra* note 12.

271. *See Hall*, 2019 WL 5892776, at *5.

272. *See Carpenter*, 138 S. Ct. at 2220; *see also* cases cited *supra* Sections IV.A–D.

273. The location information argument in the context of Zoom could be weakened, as the radius of location is broader than the ability to track within a 50-meter radius in *Carpenter*; however, as we saw in *United States v. Hood*, IP information, which is expressly stored by Zoom can, in fact, be used to determine exact location. *See* 920 F.3d 87, 91–92 (1st Cir. 2019); *Zoom Privacy Statement*, *supra* note 12.

and logout times, meeting members, chat transcripts, dictation transcripts, video recordings, etc.[274] Perhaps most importantly, Zoom, again, is only end-to-end encrypted in limited capacities.[275] Data that tracks conversations we would otherwise have in the breakroom at work or passing in the halls between classes are now neatly compiled in databases for retrospective access. For Zoom to be able to access these interactions, "subject only to [its] retention policies," should trigger Fourth Amendment protections.[276] Both FERPA and the Stored Communications Act merely require subpoenas to compel disclosure to the Government;[277] however, as the *Donovan* Court states, "subpoena[s] [must] be sufficiently limited in scope."[278] The foregoing argument demonstrates that the data collected by Zoom, just like the abundance of information collected in *Carpenter*, simply extends beyond the limited scope of a subpoena.

CONCLUSION

Moving forward, it is important for users to know whether the use of videoconferencing platforms is subject to privacy protection under the Fourth Amendment. Cases following *Carpenter* are unclear as to what standard to apply—some have reached decisions relying heavily on one factor discussed in the majority,[279] others have dismissed cases because *Carpenter* was merely a "narrow holding,"[280] and others have sought to analogize to the facts in *Carpenter*.[281] As such, it is important to know what exactly the Court will look at when determining

274. *See Zoom Privacy Statement*, *supra* note 12.

275. *See supra* Section III.B.

276. *See Carpenter*, 138 S. Ct. at 2218.

277. 34 C.F.R. § 99.31(a)(9)(i) (2012); Stored Communications Act, 18 U.S.C. § 2703(c)(2).

278. *See* Donovan v. Lone Steer, Inc., 464 U.S. 408, 415 (1984).

279. *See, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (hinging analysis on the voluntariness of turning over IP information through "making the affirmative decision to access a website or application").

280. *See, e.g.*, United States v. Hall, No. 16-CR-050-01, 2019 WL 5892776, at *5 (M.D. Pa. Nov. 12, 2019).

281. *See In re* Google Location Hist. Litig., 428 F. Supp. 3d 185, 198–99 (N.D. Cal. 2019).

whether a search into the archives of data collected by Zoom is a search protected by the Fourth Amendment. Lower courts analyzing *Carpenter* present conflicting reasoning for, or against, privacy matters. As discussed, the Massachusetts Supreme Court decision in *Almonor* upheld privacy concerns surrounding real time pinning of just a *single* location,[282] whereas the *Hood*[283] court dismissed the defendants claims because four days of location information was simply not extensive enough. Both relying on *Carpenter* to reach their decisions, the courts in these cases demonstrate precarious schemes of interpretation. Further, Zoom, like the platform analyzed in *Kidd*,[284] is not just utilized inside the home, as it is available for download on any device that supports its application.

Fourth Amendment jurisprudence is changing and will presumably continue to change as technology advances. Thus, it is vital to know what constitutes a reasonable expectation of privacy concerning information spread across our interactions over different platforms and devices. Lower courts need clearer direction than the *Carpenter* Court offered, and the above analysis demonstrates that the myriad of current interpretations is more analogous to a Jackson Pollock painting than constitutional interpretation. *Carpenter*'s "narrow" application of Fourth Amendment protection to CSLI data evaded the opportunity to recognize the shortcomings of the third-party doctrine, as there are easily identifiable and analogous circumstances involving devices ready-at-hand that extend beyond CSLI tracking.

Wherever the doctrine lands, one thing is certain: the privacy implications surrounding Zoom should widen *Carpenter*'s narrow holding to broaden the doctrine to protect videoconferencing data. The factors outlined in *Carpenter* map on to Zoom, and Justice Kennedy's concerns in the dissent are

282. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1193–94 (Mass. 2019).

283. *See Hood*, 920 F.3d at 91.

284. *See* United States v. Kidd, 394 F. Supp. 3d 357, 364–65 (S.D.N.Y. 2019).

mitigated when applying these factors to relevant technology. With respect to the first factor, Zoom is comprehensively used, as data indicates that over 300 million people are currently utilizing that platform for purposes that include employment and academia, which, given an eight-hour workday, account for nearly half the time the average person spends awake.[285] Second, to sustain social functioning in today's public health and virtual landscape, videoconferencing and technological communication is *required*, and like the CSLI in *Carpenter*, therefore falls outside any formal understanding of voluntary use.[286] Third, given the involuntary use and the comprehensiveness surrounding our use of technology, videoconferencing apps surely penetrate our most intimate spheres. Finally, as the Zoom privacy policy conveys, Zoom stores the data it collects indefinitely and gives no indication as to how long such information will be available for retrospective use.[287] Thus, if the third-party doctrine remains in place as is, the government is capable of a high degree of retrospective search patterns through Zoom.

The Court established the third-party doctrine in 1976,[288] and, since its inception, the doctrine has been pervasive in its application. But a reflection of our technological advancements should give us pause when thinking about the third-party doctrine functions today compared to the date of its inception. The VHS player was not released into US markets until 1977, the year following the Court's establishment of the doctrine.[289] Additionally, Tim Berners-Lee invented the World Wide Web in 1989, thirteen years after the doctrine opened the gates to our endeavors with third parties.[290] The doctrine predates not only

285. *See* Iqbal, *supra* note 11.

286. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

287. *See Zoom Privacy Statement*, *supra* note 12.

288. *See* United States v. Miller, 425 U.S. 435, 444–45 (1976).

289. Priya Ganapati, *June 4, 1977: VHS Comes to America*, WIRED (June 4, 2010, 12:00 AM), https://www.wired.com/2010/06/0604vhs-ces/.

290. *The Birth of the Web*, CERN, https://home.cern/science/computing/birth-web (last visited Dec. 30, 2021).

obsolete technology but has also been significantly aged by technological advancements since its inception in the 1960s. This antiquated doctrine should thus be reframed. It is time to reconsider exactly what we share with third parties and whether the same rationale—that we forfeit a right to our reasonable expectation of privacy upon relinquishing information to third parties—exists in all purviews where we sacrifice bits of data aggregating our composite endeavors. The answer? We should not.