Catholic University Law Review

Volume 69
Issue 4 *Fall 2020*

Article 8

3-22-2021

Cloudy with a Chance of Government Intrusion: The Third-Party Doctrine in the 21st Century

Steven Arango

CLOUDY WITH A CHANCE OF GOVERNMENT INTRUSION: THE THIRD-PARTY DOCTRINE IN THE 21ST CENTURY

Steven Arango[+]

Technology is unavoidable in today's world. It surrounds us daily; most of our lives require technology in some way or another. But even as society's reliance increases, privacy laws lag behind.[1] As a result, certain technologies are especially vulnerable to warrantless searches, such as cloud stored information.[2] Federal law, in the form of the Stored Communications Act (SCA), provides little safety for cloud data.[3] And the Fourth Amendment may not be any better.[4]

Although the Fourth Amendment shelters citizens' "homes, papers, and effects" from warrantless searches and seizures, the Supreme Court's third-party doctrine, which allows for "warrantless searches and seizures of information

---

[+] Steven Arango recently completed a one-year clerkship with U.S. District Judge Fernando Rodriguez, Jr. in the Southern District of Texas. He is a captain in the United States Marine Corps and currently attending The Basic School in Quantico, Virginia. Upon completion, he will report to Naval Justice School in Newport, Rhode Island. The views expressed in this Article are those of the author and do not necessarily represent the views of the U.S. Marine Corps, Department of the Navy, Department of Defense, or the U.S. Government.

A portion of this Article appeared on the American Bar Association website: https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2019/third-party-doctrine-wake-of-seismic-shift/.

1. Eric Johnson, Note, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 STAN. L. REV. 867, 870 (2017).

2. H. Brian Holland, *A Cognitive Theory of the Third-Party Doctrine and Digital Papers*, 91 TEMP. L. REV. 55, 64 (2018).

3. Johnson, *supra* note 1, at 877–78.

4. Holland, *supra* note 2, at 75.

entrusted to third parties," may overcome any constitutional protection afforded to cloud stored data.[5] When the Supreme Court established this doctrine in the 1970s, commercial cloud storage was not even a thought, let alone a reality.[6] More than 40 years later, cloud storage might be an extension of everyday society.[7] Citizens' most intimate information—from medical records to business documents—is stored on these servers.[8] As a result, broad application of the third-party doctrine by the government is an ever-growing concern.

If the third-party doctrine applies to cloud services, the government could obtain personal files with a simple subpoena or court order.[9] To obtain a subpoena, little evidence is required and, there is no judicial oversight; as long as internal policies are followed, the subpoena will generally be granted.[10] A court order requires judicial consent, but it still does not rise to the evidentiary level of warrants; a warrant requires probable cause and particularity—both of which a judge reviews.[11]

One does not have to work for the government to understand the myriad of "potential benefits of such [unencumbered] digital investigations."[12] Take your own cloud storage as an example. It probably contains photos, documents, and medical files—your "entire digital life."[13] This amount of information would take minutes to collect with a simple download; a standard investigation collecting this information could take years. For agencies that want to solve crimes quickly, what better way than to search a personal cloud account?[14]

In the coming years, there will be no shortage of third-party doctrine cases involving cloud services: "16 percent of Americans own a smart speaker" (*e.g.*,

---

5. Johnson, *supra* note 1, at 871; Aaron J. Gold, *Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software*, 56 WM. & MARY L. REV. 2321, 2322 (2015).

6. *2006: Storage in the Cloud*, THE STORAGE ENGINE (Sept. 11, 2015), https://www.computerhistory.org/storageengine/storage-in-the-cloud/.

7. Eunice Park, *Objects, Places and Cyber-Spaces Post-Carpenter: Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J. L. & TECH. 1, 16 (2019); Holland, *supra* note 2, at 73–77.

8. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

9. Vania Mia Chaker, *Your Spying Smartphone: Individual Privacy is Narrowly Strengthened in Carpenter v. United States, the U.S. Supreme Court's Most Recent Fourth Amendment Ruling*, 23 J. TECH. L. & POL'Y 1, 13–14 (2018).

10. *Id.* at 14.

11. Dylan Bonfigli, Note, *Get A Warrant: A Bright-Line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. CAL. L. REV. 307, 312 (2017); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 518 (2013).

12. Chaker, *supra* note 9, at 13.

13. *Id.*

14. *Id.*

Amazon Echo),[15] 81% of Americans own a smartphone,[16] over 500 million people are actively using Dropbox,[17] and Google Drive currently boasts one billion users.[18] Because all these devices or programs use cloud-based systems, the third-party doctrine could possibly be used to access their cloud data.[19]

As cases start to emerge, courts will turn to the recent Supreme Court case *Carpenter v. United States* for guidance.[20] *Carpenter* addressed two issues: a person's reasonable expectation of privacy in cell-site location information (CSLI) and the application of the third-party doctrine to obtain this information.[21] For Fourth Amendment protections to exist in cloud information, "users must have a reasonable expectation of privacy in their cloud stored data."[22] For brevity, this paper will assume that this requirement is met and only focus on the third-party doctrine. [23]

This Paper argues that the third-party doctrine does not apply to cloud data, and that a warrant is necessary to search and seize information stored in the cloud. To arrive at this conclusion, it first analyzed the Supreme Court's creation of the third-party doctrine and its subsequent evolution. The second part outlines cloud storage and data. The third part discusses why cloud data should be secure from warrantless searches. Lastly, this Paper explains why Congress needs to legislate this issue—not the Courts—and offers recommendations on how to do so.

I. BACKGROUND

A. Carpenter

Since the Supreme Court issued its opinion on *Carpenter*, it has received significant attention from legal scholars and for good reason. The Court's

---

15. Sarah Perez, *39 Million Americans Now Own a Smart Speaker, Report Claims*, TECH CRUNCH (Dec. 1, 2018), https://techcrunch.com/2018/01/12/39-million-americans-now-own-a-smart-speaker-report-claims/.

16. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), https://www.pewinternet.org/fact-sheet/mobile/.

17. Trefis Team, *Dropbox is Doing Well, But Looks Rich in the Face of Industry Headwinds*, FORBES (May 21, 2018), https://www.forbes.com/sites/greatspeculations/2018/05/21/dropbox-is-doing-well-but-looks-rich-in-the-face-of-industry-headwinds/#2beab95e36ed.

18. Shoshana Wodinsky, *Google Drive is About to Hit 1 Billion Users*, THE VERGE (July 25, 2018), https://www.theverge.com/2018/7/25/17613442/google-drive-one-billion-users.

19. Rob Thubron, *Apple Served with Search Warrant to Access Texas Shooter's iPhone, iCloud Account*, TECHSPOT (Nov. 19, 2017), https://www.techspot.com/news/71947-apple-%20served-search-warrant-access-texas-shooter-iphone.html.

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

21. Park, *supra* note 7, at 11–12.

22. Johnson, *supra* note 1, at 885.

23. *Id.* at 885–86; Gold, *supra* note 5, at 56 (Because *Carpenter* held that Carpenter did have a reasonable expectation of privacy for his CSLI, the Court likely would not find cloud storage users lacking this right.).

analysis revolutionized the third-party doctrine. This doctrine no longer consists of three elements but several other factors that some have argued narrow its application.[24] To be sure, the Court itself characterized *Carpenter* as a "narrow" decision.[25] But a narrow ruling should not be conflated with narrow consequences; *Carpenter*'s extension is likely far greater than most realize.[26]

1. Technological Background

At its core, *Carpenter* is about location information provided by cell phones to cell-sites.[27] Cell phones are continuously searching for the best signal, which is why they generally connect to the closest cell-site.[28] Modern phones constantly search for cell-sites even when the owner is not using the phone; all that is required is for the phone be turned on.[29] When a cell phone connects to a cell-site, "it generates a time-stamped record known as cell-site location information (CSLI)."[30] The more location information produced, the easier it is to determine someone's location.[31] Although phone companies create, collect, and store CSLI for their own business purposes, *Carpenter* explained how the government can use this information in criminal investigations.[32]

2. Factual Background

In 2011, the FBI arrested four men for a string of local robberies.[33] After being questioned by the FBI, a defendant confessed and turned over his 15 accomplices.[34] The FBI then reviewed this defendant's call records to identify other possible suspects.[35] From this evidence, the FBI learned of several other suspects, including Timothy Carpenter.[36]

Using this information, prosecutors obtained Carpenter's CSLI through the Store Communications Act (SCA), "which authorizes courts to grant orders for telecommunications records."[37] This particular section of the SCA requires a higher standard of proof than a subpoena but less than a warrant.[38] When served

24. Chaker, *supra* note 9, at 17.
25. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
26. Park, *supra* note 7, at 13; Chaker, *supra* note 9, at 17.
27. *Carpenter*, 138 S.Ct. at 2211–12.
28. *Id.*
29. *Id.* at 2211.
30. *Id.*
31. *Id.* at 2211–12.
32. *Id.* at 2212.
33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.*; Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485, 533–34 (2018).
38. *Carpenter*, 138 S. Ct. at 2210.

with this court order, Carpenter's wireless carriers provided CSLI for the specific "four-month period when the string of robberies occurred."[39] This information helped prove that Carpenter was near the robberies when they occurred; although his CSLI could only show his whereabouts "between a half mile and two mile" radius.[40] That said, the FBI used this evidence to charge Carpenter with aiding and abetting robbery.[41]

Carpenter argued that the warrantless seizure of his CSLI violated his Fourth Amendment rights, and that the evidence should have been suppressed.[42] Both lower courts rejected this argument, and the appellate court explained that when Carpenter shared his CSLI to these third-parties, he waived any Fourth Amendment rights attached to the information.[43]

3. Majority Opinion[44]

In *Carpenter*, the sole issue was whether the government violated the Fourth Amendment when it accessed Carpenter's CSLI without a warrant.[45] Although CSLI is held by a third-party, the Court explained that the "unique nature" of this information outweighed this outside control.[46] For this reason, the Court held that Carpenter's CSLI still possessed Fourth Amendment protections.[47] How the Court arrived at this conclusion is what matters for future third-party doctrine cases.

Carpenter discussed the third-party doctrine at length and reconfigured its meaning.[48] But before one can understand how *Carpenter* changed this doctrine, the two cases that helped create it must be considered: *United States v. Miller*[49] and *Smith v. Maryland*.[50]

Miller established the third-party doctrine.[51] It held that once an individual voluntarily turned over documents to a bank—they became the bank's business records—and a constitutional privacy interest ceased to exist in the documents.[52] Once the bank had these records, they were used in the bank's "ordinary course

39. *Id.* at 2212.
40. *Id.* at 2212–13, 2225 (Kennedy, J., dissenting).
41. *Id.* at 2212.
42. *Id.*
43. Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 217–18 (2018).
44. *Carpenter*, 138 S. Ct. at 2206, 2211.
45. *Id.* at 2212.
46. *Id.* at 2217.
47. *Id.*
48. *Id.* at 2216–17, 2219–22.
49. United States v. Miller, 425 U.S. 435 (1976).
50. Smith v. Maryland, 442 U.S. 735 (1979).
51. *Miller*, 425 U.S. at 444.
52. *Id.*

of business."[53] Important to *Miller's* analysis was that the bank was not simply an intermediary for these transactions but a necessary party.[54] And the documents, which were created for commercial transactions, underscored Miller's reduced expectation of privacy.[55]

Miller's belief that the documents would be "used only for a limited purpose" did not help him reclaim his lost Fourth Amendment protections.[56] When Miller voluntarily exposed his information to the bank, he assumed the risk that the bank would provide the information to the government.[57] Thus, he no longer held an expectation of privacy in the documents.[58]

Smith[59] applied the same doctrine a few years later. In *Smith*, the government used a pen register to record phone numbers dialed on a landline telephone.[60] The Court ruled that the third-party doctrine applied, and that this action did not constitute a search.[61] Telephone users generally know that dialed numbers are conveyed to phone companies and recorded for "legitimate business purposes."[62] In like manner, most people are aware of pen registers' existence and functions.[63] *Smith* also explained that the technology used here by law enforcement provided only "limited capabilities"; they could only access the numbers dialed, not the content of the call, limiting the information gathered to the parties' identities.[64] As a result, Smith did not have a reasonable expectation of privacy in his dialed phone numbers.[65]

In short, *Miller* and *Smith* applied a doctrine that allows the government to obtain information without a warrant from a third-party if: "(1) information [is] voluntarily disclosed (2) for use by a third-party (3) in its normal course of business."[66] Until *Carpenter*, if these elements were met, the third-party doctrine could apply.[67] But *Carpenter* not only expanded the meaning of some of the original elements, it also created new factors for consideration.

---

53. *Id.* at 442–43.
54. *Id.*
55. *Id.*
56. *Id.* at 443.
57. *Id.*
58. *Id.*
59. Smith v. Maryland, 442 U.S. 735 (1979).
60. *Id.* at 737.
61. *Id.* at 742–44.
62. *Id.* at 743 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.").
63. *Id.* at 742.
64. *Id.* at 742–43.
65. *Id.* at 744.
66. Johnson, *supra* note 1, at 883.
67. *Id.*

Because Carpenter revealed his location to his wireless providers, the government argued that the third-party doctrine provided access to this information.[68] Undeniably, Carpenter provided information to a third-party, his wireless carriers, which used this information in their normal course of business.[69] For that reason, the second and third elements were met.[70] But the Court reasoned that Carpenter did not voluntarily share this information, failing the first element of the third-party doctrine.[71] As part of its analysis of this element, *Carpenter* focused on the essential role of cell phones in today's society and Carpenter's awareness of how wireless carriers collected CSLI.[72]

Cell phones are integral to modern society.[73] People use cell phones for many reasons: to set their calendars, to work on documents, to call co-workers, friends, and family.[74] Without cell phones, people would not have meaningful participation in society.[75] And because of this essentialness, the owner is stripped of a voluntary choice on whether to own a cell phone; by extension, the owner does not voluntarily share his CSLI either.[76]

Awareness shared a similar fate. As long as a cell phone is on, it will continuously connect to local cell-sites.[77] So the only affirmative act necessary to create CSLI is turning the phone on.[78] And the only way to avoid CSLI collection is to disconnect the phone from the network.[79] *Carpenter* explained that users do not intentionally turn over "a comprehensive dossier of [their] physical movements" by the simple act of leaving their phone on.[80] Unlike Miller and Smith's affirmative acts that provided the information, the wireless carriers in *Carpenter* received the information automatically following a simple, unrelated act.[81] Turning a phone on does not create an awareness that CSLI is being collected; it is generally understood that bank documents are used for commercial transactions and phone providers record phone numbers for business purposes.[82]

---

68. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).
69. *Id.* at 2217.
70. *Id.*
71. *Id.* at 2220. The United States is home to 70 million more cell phone accounts than people. *Id.* at 2211.
72. *Id.* at 2220.
73. *Id.* at 2218.
74. *Id.* at 2262 (Gorsuch, J., dissenting).
75. *Id.* at 2220.
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*

Carpenter did not only rely on the original elements of the third-party doctrine to reach its conclusion.[83] As the Court explained, although a reduced constitutional expectation of privacy exists when "information [is] knowingly shared with another," this fact is not dispositive in third-party cases.[84] *Carpenter* established three new third-party factors: (1) the scope of the personal information accessed, (2) the nature of the information accessed, and (3) the technological features of the respective technology.[85]

Carpenter's scope of information exceeds the information at issue in previous Supreme Court third-party doctrine cases. *Miller* and *Smith* granted access to "limited types of personal information."[86] But Carpenter's CSLI provided a window not only into the defendant's location but also his personal life.[87] Smith's landline provider could only record the numbers dialed; through CSLI, wireless providers not only receive the numbers dialed by the user but also a "detailed and comprehensive record of the person's movements."[88] With a few inferences, where someone travels can provide insight into their "familial, political, professional, religious, and sexual associations."[89] And because a cell phone is basically an extension of the human body—it travels everywhere.[90]

But the scope of information is not confined to present movements or associations.[91] Wireless carriers maintain CSLI for up to five years, which provides a retrospective surveillance no other technology or person can offer.[92] And if this information is properly interpreted, the government can learn a person's past, present—and maybe—future movements.[93] Although not the equivalent of the surveillance in George Orwell's "1984,"[94] this development is still concerning.[95]

The second factor examined the nature of the information that Carpenter provided his wireless carriers.[96] *Carpenter* noted that "CSLI is an entirely different species of business record" than the bank documents in *Miller* or the

---

83. *Id.* at 2219 ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

84. *Id.*

85. Holland, *supra* note 2, at 97.

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

87. *Id.*

88. *Id.* at 2217.

89. *Id.* at 2217.

90. *Id.* at 2218.

91. *Id.*

92. *Id.*

93. *Id.*

94. *See generally* GEORGE ORWELL, 1984 (1949).

95. *Carpenter*, 138 S. Ct. at 2218 ("Only the few without cell phones could escape this tireless and absolute surveillance.").

96. Holland, *supra* note 2, at 97.

phone log in *Smith*.[97] Both Miller and Smith revealed little identifying information, and Smith revealed no content .[98] But CSLI provides sensitive and revealing information—a window into the "privacies of life."[99] Simply put, an exhaustive location record is quite different than a few bank documents or a phone log.[100]

Carpenter's last factor focused on the technology behind CSLI.[101] The pen register in *Smith* provided limited capabilities; the police could see the number dialed, but the content remained private.[102] In contrast, the government in *Carpenter* could deduce Carpenter's location and associations with his CSLI.[103] And soon CSLI will be able to pinpoint one's location, like GPS.[104] Moreover, this technology allows continuous monitoring when a phone is on; a pen register only collects information when a phone call is made.[105] Lastly, CSLI's technology provides access to this information in a "remarkably easy, cheap, and efficient [manner] compared to traditional investigative tools."[106] Information that would usually take years to gather can be obtained in minutes—at essentially no cost.[107]

The Court's focus on these new factors suggests that it felt uncomfortable extending this doctrine to exceedingly personal and revealing information.[108] But even though *Carpenter* held that the FBI needed a warrant to obtain the CSLI, it also warned that this decision was a narrow one.[109] Depending on how future courts interpret this holding, warrantless searches of cloud storage accounts could be possible.

B. Cloud Storage

Cloud storage provides users with the ability to upload files through the internet and store them offsite in a third-party owned and operated server.[110] Storage services, such as Dropbox or Google Drive, require users to create an account before uploading their files.[111] Once files are uploaded, they will remain

97. *Carpenter*, 138 S. Ct. at 2222.
98. *Id.* at 2219.
99. *Id.* at 2217–19; Holland, *supra* note 2, at 97.
100. *Carpenter*, 138 S. Ct. at 2219.
101. Holland, *supra* note 2, at 97.
102. *Carpenter*, 138 S. Ct. at 2219.
103. *Id.* at 2217.
104. *Id.* at 2217–18.
105. *Id.* at 2217.
106. *Id.* at 2217–2218.
107. *Id.*
108. *Id.* at 2217–19; Chaker, *supra* note 9, at 10.
109. *Carpenter*, 138 S. Ct. at 2220.
110. Johnson, *supra* note 1, at 872.
111. *Id.* at 892.

on the servers as long as the account remains active.[112] Some providers also allow users to edit, share, and copy their files on the cloud, providing a cloud computing component.[113]

Although most cloud services are password protected, most lack encryption.[114] Password protection still permits storage providers to access the information.[115] And even if the service offers an encryption option, encryption does not always provide absolute protection. Data can still be backed up on other servers, which would allow the provider to access the information.[116] If the provider does so, depending on the terms of service, it may collect or scan the information for "business purposes."[117]

The information collected from stored files comes from two main sources: data and metadata.[118] To illustrate, consider a Word document. The words within the document are data; the "origin, purpose, time, geographic location, creator, access, and terms of use of the data" are all metadata.[119] In essence, metadata is "data about data."[120] As metadata increases over time, it "can be more telling than the content" of the respective files.[121] Metadata can reveal a "detailed account of one's interests, activities, and associations."[122] And even if a file is deleted, the "deleted data still remains in the cloud for a certain period of time."[123]

Some service providers also collect other information not associated with uploaded files.[124] This information includes the previous website visited before using the cloud service, "the device and software used to access the service," and the searches within the cloud program.[125] This information coupled with

---

112. *Id.* at 873.

113. *Id.*

114. *Id.*

115. *Id.* at 873–74.

116. Johnson, *supra* note 1, at 873–74.

117. Holland, *supra* note 2, at 73–75; Johnson, *supra* note 1, at 873–74.

118. Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 274–75 (2016).

119. *Data Documentation and Metadata*, U. ARIZ. LIB., https://data.library.arizona.edu/data-management-tips/data-documentation-and-metadata (last visited Mar. 7, 2020).

120. Thomas H. White, *Parol Metadata: New Boilerplate Merger Clauses and the Admissibility of Metadata Under the Parol Evidence Rule*, 4 J.L. TECH. & INTERNET 237, 237 n.1 (2012); *Metadata Creation*, U.C. SANTA CRUZ U. LIBR., https://guides.library.ucsc.edu/c.php?g=618773 (last visited Mar. 7, 2020).

121. Price, *supra* note 117, at 275–76.

122. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473, 485 (2016).

123. Sarit K. Mizrahi, *The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users During the Course of Criminal Investigations in Canada and the United States*, 25 TUL. J. INT'L & COMP. L. 303, 320–21 (2017).

124. Scott A. McDonald, *Authenticating Digital Evidence from the Cloud*, ARMY LAW. 40, 48 (2014).

125. *Id.*

the data and metadata from uploaded files could provide the government with an unprecedented look into someone's life.[126]

II. ANALYSIS

A. Cloud Information Should Be Secure from Warrantless Searches

For the third-party doctrine's voluntary element, *Carpenter* focused on two issues: (1) the essential role cell phones hold in today's society and (2) Carpenter's awareness of how his wireless carriers collected his CSLI.[127] Because cell phones are a social necessity, *Carpenter* explained that mere ownership of a cell phone does not suggest CSLI is voluntarily shared.[128]

But is cloud storage necessary to engage in modern life? It has certainly experienced a "wide social adoption" like cell phones.[129] And much of personal information has shifted from personal storage to remote cloud storage.[130] In fact, users are being forced to use cloud services because they are producing more data than their devices can store, and cloud storage is the best option available.[131]

Moreover, the alternatives to cloud storage do not eliminate the cloud's essentialness.[132] Although external hard drives offer many of the same functions as cloud services, their accessibility is inadequate in comparison.[133] External hard drive access is limited to the physical device itself, and generally, only one person can connect to the specific device.[134] By contrast, many users can access cloud information in real-time.[135]

---

126. Price, *supra* note 117, at 275–76.

127. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

128. *Id.*

129. Park, *supra* note 7, at 16; Holland, *supra* note 2, at 73–75 (Because *Carpenter* does seem to equate total number of users with essentialness, the significant number of cloud users could be dispositive for this question).

130. Aya Hoffman, *Lost in the Cloud: The Scope of the Private Search Doctrine in a Cloud-Connected World*, 68 SYRACUSE L. REV. 277, 286 (2018); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 739–41 (2016).

131. Diamantis, *supra* note 36, at 503–04; Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 161 (2014).

132. Stalina Zoir, *Cloud Storage vs External Hard Disk Drive: Which One is Better?*, TECH RADAR (June 18, 2018), https://www.techradar.com/news/cloud-storage-vs-external-hard-disk-drive-which-one-is-better.

133. *Id.* Lincoln Specter, *Cloud Storage Alternatives: Three Ways to Sync Your Own Data Securely and Privately*, PC WORLD (July 30, 2015), https://www.pcworld.com/article/2940646/cloud-storage-alternatives-three-ways-to-sync-your-own-data-securely-and-privately.html (discussing other storage options).

134. Adam W. Snukal et al., *Cloud Computing—Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing, Part One*, 65 CONSUMER FIN. L.Q. REP. 57, 58 (2011); Mark Wilson, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U. L. REV. 261, 263 (2013).

135. Wilson, *supra* note 133, at 263.

Without general access, external hard drives force users to share stored data by email, flash drive, or using the same device.[136] Imagine having to carry this device everywhere you went, sitting down, plugging it into your laptop, downloading documents from it, and then sharing those documents by email. Now imagine going through this process every time you needed to share files from your external hard drive. This method is unrealistic in today's world. And what if the file is too large to share by email? Gmail only allows emails to contain files below 25 megabytes, and most other email providers have a stricter data limit.[137] Today's world requires speed, access, and reliability—only the cloud can provide all three of these features.[138] Cloud storage is not merely beneficial to everyday life, it is essential.[139]

The second issue considers a cloud user's awareness that their data is collected. In effect, does uploading files to a cloud service create an awareness that this information is being collected? People who turn over bank documents or make phone calls generally know that the information from their documents or phone numbers are collected.[140] Banks and phone companies have to record this information for business purposes. But other than the terms of service, there is no reason cloud users would know that their data is being collected.[141] Uploading files to a cloud service is like Carpenter's act of leaving his phone on—neither create an awareness that companies are collecting the information the individual created.[142] Because of the cloud's essentialness and the user's lack of awareness that their data is collected, cloud users do not voluntarily share their data with cloud providers.

The third-party doctrine's second and third elements require a third-party to use the information collected for business purposes.[143] Depending on the terms of service offered by the cloud provider, the user's data may not be "used" in the sense *Carpenter*, *Miller*, or *Smith* understood this term to mean.[144] Terms of service define "the amount of privacy the user relinquishes", and we must be careful not to conflate access with use.[145] Some providers will scan uploaded

136. Daniel E. Harmon, *The State of Data Storage*, 34 No. 6 LAWPC 1, 1–2 (2016).

137. *Maximum Email Size Limit for Gmail, Outlook.com, etc.*, OUTLOOK APPS (July 19, 2013), https://www.outlook-apps.com/maximum-email-size/.

138. Bryan R. Kelly, *#privacyprotection: How the United States Can Get its Head Out of the Sand and into the Clouds to Secure Fourth Amendment Protections for Cloud Journalists*, 55 WASHBURN L.J. 669, 696–97 (2016); Serafino, *supra* note 130, at 161; Wilson, *supra* note 133, at 279 ("It's no answer to suggest . . . that people can avoid these hazards by not storing their data electronically.").

139. Hoffman, *supra* note 129, at 286; Serafino, *supra* note 130, at 172–173.

140. Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 438 (1976).

141. Johnson, *supra* note 1, at 891.

142. *Id.* at 891–92.

143. *Id.* at 883.

144. *Id.* at 895–96; Gold, *supra* note 5, at 2342–43.

145. Johnson, *supra* note 1 at 898–99; Gold, *supra* note 5, at 2342–43.

cloud data "for the security, stability, and control of the network", while other providers will not only have access to the data but use information from this data.[146] If cloud providers use the data pulled from uploaded files for business purposes, the third-party "usage" requirement would be met.[147] But if the cloud provider simply scans the information, this element would not be satisfied.

Carpenter's first new factor considered the scope of the personal information accessed.[148] At any time, a cloud user may upload and store receipts, medical files, personal photos, and business documents to their account.[149] Although CSLI cannot provide specific location, metadata can.[150] Both metadata and data can reveal a person's "familial, political, professional, religious, and sexual associations."[151] And unlike CSLI, few to no inferences need to be made to understand this information.[152] But much like the retrospective aspect of CSLI, even after a file is deleted, its data can remain in the cloud.[153]

Carpenter's second factor focused on the nature of the information accessed.[154] The nature of information provided by cloud data is inherently sensitive and revealing, which is why storage providers offer password protected access and, sometimes, encryption.[155] But cloud information "is an entirely different species of business record" than CSLI.[156] CSLI cannot provide the type of personal information that cloud data can; cloud data can provide someone's "entire digital life," their specific location, and many other details—all requiring few to no inferences to understand the data.[157] By contrast, CSLI can only show someone's location within "a half mile and two mile" radius.[158] And without inferences or other evidence, this information is useless.[159]

Carpenter's last factor examined the various technological features underlying the respective software.[160] Some cloud providers' terms of service

146. Johnson, *supra* note 1, at 873.

147. *Id.* at 903.

148. Holland, *supra* note 2, at 97–99.

149. Keane Woods, *supra* note 129, at 739 n.47.

150. Orin S. Kerr, The Digital Fourth Amendment: Implementing *Carpenter*, Oxford University Press, 44–45 (forthcoming) (on file at https://ssrn.com/abstract=3301257).

151. Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018); Diamantis, *supra* note 36, at 498–99.

152. *Id.*

153. Mizrahi, *supra* note 122, at 320–21.

154. Holland, *supra* note 2, at 97–99.

155. Keane Woods, *supra* note 129, at 739 n.47.

156. *Carpenter*, 138 S. Ct. at 2222.

157. Chaker, *supra* note 9, at 13–14; Kerr, *supra* note 149, at 14; David A. Harris, *Riley v. California and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 923–25 (2016).

158. *Carpenter*, 138 S. Ct. at 2225.

159. *Id.*

160. Holland, *supra* note 2, at 97–99.

and software allow them to access personal cloud data.[161] Terms of service can permit even more access, allowing for automated uploads and the "pervasive collection of information."[162] Either way, government access to this information has the power to make traditional investigative tools obsolete.[163] Cloud data is centrally located, extensive, and requires little effort to collect.[164] But most importantly, its access is cheap—no wiretaps, extra agents, or overtime are necessary to gather it—just a simple data request.[165] Like *Carpenter*, this type of technology provides access to information "on a scale that was not technologically feasible a short while ago."[166]

Overall, cloud data shares more similarities with *Carpenter* than *Miller* or *Smith*. Cloud storage is essential, and users are unaware that their information is collected after they upload files. Thus, the voluntary element is not met. Depending on the terms of service, the data might not be used by the cloud provider. However, most cloud services do use customers' data for business purposes.[167] Therefore, this element would likely be met. Even so, the scope of personal cloud information and its nature are more extensive and sensitive than CSLI's scope and nature. Moreover, cloud technology mirrors the technology behind CSLI.[168] As a result, after *Carpenter*, the third-party doctrine should not apply to cloud storage services.[169]

B. Congress's Role

More than 40 years ago the Supreme Court created the third-party doctrine.[170] At its inception, it was impossible for any judge—even Supreme Court Justices—to appreciate how society's reliance on technology would create a "seismic shift" in the doctrine's reach.[171] Consider the fact that it was not until 30 years after *Miller* established the third-party doctrine that cloud storage became commercially available.[172] And by no means was its use as prevalent as it is today.[173] The Court tried to rein in the doctrine's reach with *Carpenter*; perhaps it did. But until courts address warrantless searches of cloud data, it is

161. Gold, *supra* note 5, at 2342–43; Johnson, *supra* note 1, at 895–96.

162. Holland, *supra* note 2, at 97–99.

163. *Id.* at 497–98.

164. *Id.*

165. Diamantis, *supra* note 36, at 497–98.

166. *Id.* at 498–99.

167. Johnson, *supra* note 1, at 909.

168. Diamantis, *supra* note 36, at 497–98.

169. Johnson, *supra* note 1, at 895.

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

171. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

172. *2006: Storage in the Cloud*, THE STORAGE ENGINE (Sept. 11, 2015), https://www.computerhistory.org/storageengine/storage-in-the-cloud/.

173. *Id.*

pure speculation whether this data retains Fourth Amendment protections. To wait and hope for favorable application of *Carpenter* in these cases is to gamble with each individual's cloud privacy.

Instead, Congress needs to address cloud privacy with legislation.[174] Cloud storage is a highly complicated area that requires a depth of fact-finding and deliberating not suited for the judicial system.[175] Of course, Congress has not always been reliable at legislating technological issues, but Congress's struggles should not provoke a judicial response.[176]

Statutes provide much more latitude and stability than judicial precedent.[177] Statutes can require notice to the individual affected by the search, which gives them the ability to respond through legal channels.[178] Statutes can require a higher standard of proof than warrants, such as clear and convincing evidence.[179] Statutes can create exceptions. For example, national security issues are exempted from the SCA's requirements.[180] Finally, statutes can control the government's use and storage of seized data.[181] But the judiciary usually can only "regulate [the] acquisition of information."[182] At their core, statutes provide broader, more stable protections than judicial precedent.[183]

Regrettably, only a small portion of cloud stored data is protected by federal law, specifically the SCA.[184] Congress developed the SCA in the 1980s when commercial cloud usage was not a reality.[185] As a result, Congress created a framework that protected the only privacy concern at the time—electronic communications.[186]

If cloud based data does not involve electronic communications, it is not protected.[187] Suppose you upload a spreadsheet with all your financial information to Dropbox—this type of information would not be protected by the SCA because there is no communication involved. But if a Gmail account

174. Murphy, *supra* note 11, at 489.

175. *Id.* at 489.

176. *Id.* at 533.

177. *Id.* at 537.

178. *Id.* at 535.

179. *Id.* at 535.

180. Diamantis, *supra* note 36, at 500; Serafino, *supra* note 130, at 191–92 ("FISA is considered exempt from the probable cause requirement because it is aimed at preventing terrorism, not just ordinary criminal wrongdoing.").

181. *Id.* at 537.

182. *Id*. at 535.

183. *Id.* at 540.

184. Gold, *supra* note 5, at 2333.

185. *2006: Storage in the Cloud*, THE STORAGE ENGINE (Sept. 11, 2015), https://www.computerhistory.org/storageengine/storage-in-the-cloud/.

186. Johnson, *supra* note 1, at 877.

187. Gold, *supra* note 5, at 2333.

backed up emails into Google Drive, this information would be protected.[188] In effect, the SCA does not protect most cloud data.[189]

To address cloud privacy, Congress needs to expand the SCA to protect non-communicative cloud data. Requiring probable cause and a warrant to access this information would be a welcomed change. But the "procedural protections" are what matter for cloud privacy, not the document required to obtain the information, such as a warrant or subpoena.[190] Congress should require probable cause and notice to acquire personal cloud data. It should also create safeguards to prevent the "unauthorized exposure" of data and compel its destruction after its use.[191] Lastly, it should expand the national security exemption to cover these requirements.[192]

The government would violate this statute if it searched a personal cloud account or used seized information without meeting these requirements. The trigger for this statute may "over-protect [digital] records"—but it is better to over-protect than under-protect this type of information.[193] And transparency and clarity are the hallmark of a well-written statute.[194] Without these features, confusion and abuse are inevitable.[195] Employing this concrete standard reduces the chance of either occurring.[196] Some may argue that this standard is too rigid. But suppose law enforcement enters your house without a warrant and searches your desk. Clearly, this type of entry and search is unlawful.[197] Why should personal cloud information be any different?

A legislative fix would also clarify this issue for defendants, prosecutors, and private companies.[198] Defendants would know their rights; prosecutors would know their boundaries; and cloud providers would know when it was necessary to comply with the government.[199] As long as this area remains unlegislated, companies and individuals will face expensive litigation and difficult decisions.[200] Cloud providers do not want customers losing faith in their service,

---

188. *Id.* at 2333–34.

189. Johnson, *supra* note 1, at 877; Matthew McKenna, *Up in the Cloud: Finding Common Ground in Providing for Law Enforcement Access to Data Held by Cloud Computing Service Providers*, 49 VAND. J. TRANSNAT'L L. 1417, 1430 (2016); Serafino, *supra* note 130, at 185.

190. Murphy, *supra* note 11, at 518–19.

191. *Id.* at 520–21.

192. *Id.*

193. Orin S. Kerr, The Digital Fourth Amendment: Implementing *Carpenter*, Oxford University Press, 28 (forthcoming) (on file at https://ssrn.com/abstract=3301257).

194. *Id.*

195. *Id.* at 26; MICHAEL CHERTOFF, EXPLODING DATA: RECLAIMING OUR CYBER SECURITY IN THE DIGITAL AGE 200 (Atlantic Monthly Press, 2018).

196. Kerr, *supra* note 149, at 28.

197. *Id.*

198. Murphy, *supra* note 11, at 535–36.

199. *Id.*

200. *Id.* at 536.

which is why they are likely to oppose data requests.[201] But a federal statute provides "legal safe harbors for compliance[,]" freeing companies from difficult ethical decisions and angry customers.[202]

Even with a privacy statute that protects cloud information, Congress must do more. Congress needs to create a law that forces it to revisit digital privacy statutes on a recurring basis. Keeping pace with rapid technological changes will not be easy.[203] Finding bipartisan support for these laws may be an even greater hurdle. But with the constant evolution of technology, using 30-year-old statutes for digital privacy is a recipe for disaster. With this law, Congress will be forced to examine digital privacy protections more than every 30 years.

III. CONCLUSION

Digital privacy is threatened without statutory protection.[204] To be sure, the government should have "the appropriate legal authority to provide security" and fulfill its constitutional role.[205] At the same time, people must maintain "a sufficient scope of privacy and autonomy necessary for [their] human dignity."[206] Here lies the inherent tension. But the recommendations put forth by this paper accommodate both essential principles.

For those that argue that these suggestions will allow people to "do things they shouldn't be doing[,]" I respectfully disagree.[207] The proposed statutory amendment "allow[s] people to live core areas of their personal lives with the dignity that excludes onlookers."[208] The United States is not a totalitarian country.[209] We have always warned against oppressive behavior in the physical world, and the digital world should be no different. Armed with wholesale cloud access, the government could "pursue personal vendettas, target the politically unpopular," and trample on other civil liberties.[210]

---

201. *Id.*
202. *Id.*
203. *Id.* at 540–41.
204. Holland, *supra* note 2, at 58.
205. CHERTOFF, *supra* note 194, at 199.
206. *Id.*
207. Diamantis, *supra* note 36, at 501.
208. *Id.*
209. *Id.*
210. CHERTOFF, *supra* note 194, at 200; KERR, *supra* note 149, at 26; Diamantis, *supra* note 36, at 501; Johnson, *supra* note 1, at 869–70. The U.S. government has controversially surveilled individuals and groups in the past:

> In 1963, the Federal Bureau of Investigation wiretapped the phones of Martin Luther King, Jr. under the pretense of determining King's ties to members of the American Communist Party. And after 9/11, the New York Police Department, with significant assistance from the Central Intelligence Agency, spent years monitoring Muslim neighborhoods and community centers.

Johnson, *supra* note 1, at 869–70.

Since 9/11, the government has received "greater investigative latitude" but extending this ability to warrantless searches of cloud services is unwise.[211] Although *Carpenter* appears to protect cloud data from warrantless searches, this area is still "ripe for future Supreme Court review."[212] And so, Congress must act.

211. Chaker, *supra* note 9, at 13.
212. *Id.*