Washington Law Review

Volume 96 | Number 1

3-1-2021

Revising Reasonableness in the Cloud

Ian Walsh

REVISING REASONABLENESS IN THE CLOUD

Ian Walsh*

Abstract: Save everything—just in case—and search for it later. This is a modern mantra fueled by the ubiquity of smartphones, laptops, tablets, and free or low-cost data storage that leads users to store massive amounts of data in the cloud. But when users trust third-party cloud storage providers with private communications, they also surrender Fourth Amendment constitutional certainty. Existing statutory safeguards for these communications are lower than Fourth Amendment warrant and probable cause standards; this permits the government to seize large quantities of users' private communications stored in the cloud with only minimal justification. Due to the revealing nature of such communications, the existing protections for them are insufficient under the Fourth Amendment. To prevent broad intrusions into users' reasonable expectation of privacy, this Comment proposes an approach akin to *Berger v. New York*, where the Supreme Court invalidated a statute that allowed invasive real-time eavesdropping because the statute did not require sufficient particularization. Like in *Berger*, seizures of private communications in the cloud should require a warrant based on probable cause that is sufficiently particularized to protect against indiscriminate, large-scale data collection and roving searches by the government.

INTRODUCTION

Approximately 266 million people in the United States own smartphones—accounting for 81% of Americans.[1] The United States Supreme Court has observed that modern cell phones store "a digital record of nearly every aspect of their [users'] lives—from the mundane to the intimate" and are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[2]

The convenience and ubiquity of modern devices result from technological developments that enable fast communication and high-capacity storage, provided through online platforms run by third parties

---

* J.D. Candidate, University of Washington School of Law, Class of 2021. Special thanks to Professor Mary Fan for her helpful guidance and insightful edits. I would also like to thank the entire *Washington Law Review* editorial staff for their invaluable assistance, especially Oliana Luke, Monica Romero, and Quynh La.

1. The population of the United States was estimated to be 328,239,523 in 2019. Press Release, U.S. Census Bureau, 2019 U.S. Population Estimates Continue to Show the Nation's Growth Is Slowing (Dec. 30, 2019), https://www.census.gov/newsroom/press-releases/2019/popest-nation.html [https://perma.cc/TJ8K-N3CE]. Multiplying this population by estimated smartphone ownership of 81% equals 265,874,013 people. *See Mobile Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/8VSE-GMNZ].

2. Riley v. California, 573 U.S. 373, 385, 395 (2014).

such as Apple and Google.[3] Use of these platforms is colloquially known as storing data in "the cloud."[4] Users store much of the personal data from their smartphones and computers in the cloud.[5] But when users share data with third-party cloud storage providers, they may surrender Fourth Amendment constitutional protection.[6]

The Fourth Amendment safeguards people and their effects from "unreasonable searches and seizures."[7] The framers of the Constitution established this protection to repudiate the colonial-era English practice of using general warrants to conduct invasive and unjustified searches for evidence of possible wrongdoing.[8] To limit the authority of officers, the Fourth Amendment requires that warrants be founded on probable cause and describe with particularity both the "place to be searched" and the "persons or things to be seized."[9]

However, the Fourth Amendment's reach has been limited when information is disclosed to third parties.[10] This is significant because modern devices rely on third-party cloud platforms for data storage.[11] Smartphones use cloud storage for a variety of features, including backing up important data.[12] Computers also often incorporate cloud platforms such as OneDrive, Google Drive, and Dropbox to provide convenient cross-device access.[13] The integration of these platforms with a wide array of devices means that users both wittingly and unwittingly store data with vast depth and breadth in the cloud.[14]

Given the limitations of the Fourth Amendment, the primary protection for private communications stored in the cloud is a statute called the Stored Communications Act (SCA).[15] The SCA was enacted in 1986—

---

3. *See infra* Part I.

4. *See What Is the Cloud?*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/overview/what-is-the-cloud/ [https://perma.cc/UT4C-NGCJ] ("Instead of accessing files and data from a local or personal computer, you are accessing them online from any Internet-capable device—the information will be available anywhere you go and anytime you need it.").

5. *See infra* section I.B.

6. *See infra* section II.B.

7. U.S. CONST. amend. IV.

8. *See infra* section II.A.

9. U.S. CONST. amend. IV; *see infra* section II.A.

10. *See infra* section II.B.

11. *See infra* section I.B.

12. *See infra* section I.B.

13. *See infra* section I.B.

14. *See infra* section I.B.

15. *See* 18 U.S.C. §§ 2701–13. The statute was first enacted as part of the Electronic Communications Privacy Act (ECPA). *See* Electronic Communications Privacy Act of 1986, Pub. L.

over thirty years ago—and permits the government to obtain information stored in the cloud using standards that fall below Fourth Amendment baselines.[16] In the context of private communications stored in the cloud, these lower standards conflict with the framers' abhorrence of unreasonable general warrant searches and seizures that motivated the Fourth Amendment's adoption.[17]

What constitutes an unreasonable search or seizure changes as technology progresses.[18] Over the past twenty years alone, the Supreme Court has addressed the privacy impacts from thermal imaging of homes, searches of phones incident to arrest, and cell site location data.[19] In 1967, the Court confronted the then-modern technological innovation of real-time wiretapping in *Berger v. New York*.[20] This decision recognized that the privacy invasion from real-time eavesdropping on telephone conversations through wiretapping, if left unchecked, would be the functional equivalent of general warrant searches.[21] The Court was especially concerned because the New York statute that authorized eavesdropping did not require a warrant or sufficient particularization and instead gave officers "a roving commission to 'seize' any and all" communications.[22] To prevent invasive general-warrant-like seizures, the Court required a warrant—based on probable cause—and "precise and discriminate" particularization procedures.[23]

Today, Americans face a privacy threat akin to wiretapping in the form of government searches and seizures of private communications stored in the cloud. To effectively safeguard a reasonable expectation of privacy for Americans, this Comment proposes a *Berger*-like Fourth Amendment approach.[24] A warrant that is supported by probable cause should be

---

No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). It has been referred to by various names, including "Chapter 121" and "Title II"; for simplicity, this Comment refers to this statute as the "Stored Communications Act" or "SCA." *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 n.1 (2004).

16. *See infra* section II.C.

17. *See infra* section I.B; *infra* Part IV.

18. *See* Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2214 (2018) (interpreting the Fourth Amendment to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

19. *See Kyllo*, 533 U.S. at 34–35 (thermal imaging); Riley v. California, 573 U.S. 373, 401–02 (2014) (cell phones incident to arrest); *Carpenter*, 138 S. Ct. at 2217 (cell site location information).

20. 388 U.S. 41 (1967).

21. *See id.* at 59.

22. *Id.*

23. *Id.* at 58–59.

24. *See infra* Part IV.

required.[25] Additionally, because of the broad scope of the intrusion and the highly revealing nature of information stored in the cloud, the warrant should be subject to "precise and discriminate" enhanced particularization requirements that minimize the scope of the seizure.[26] This enhanced particularization heeds the repeated call of the Supreme Court to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[27] Like with *Berger*, Congress should recognize technology's power to undermine privacy and enact a comprehensive statute that exceeds this constitutional baseline.[28]

This Comment proceeds in four Parts. Part I outlines how modern technological advances have impacted the invasiveness of searching and seizing communications from cloud storage platforms.[29] Part II evaluates the existing protections from such seizures, both constitutionally and statutorily, and explains some of their limitations.[30] Part III explores how the Supreme Court has confronted various intrusive technological advancements in the past.[31] Part IV then proposes a *Berger*-like approach to protect a reasonable expectation of privacy in the cloud that should be a constitutional backstop to any new statutory framework.[32]

I. TECHNOLOGY ENCOURAGES USERS TO STORE VAST AMOUNTS OF DATA IN THE CLOUD

Most people in the United States own a smartphone that depends on software made by either Apple or Google.[33] Both companies provide built-in online storage platforms for these devices that encourage users to store important and highly personal information in the cloud.[34] The

25. *See infra* section IV.A.

26. *See Berger*, 388 U.S. at 58–59; *infra* section IV.B.

27. *See* Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2214 (2018); Kyllo v. United States, 533 U.S. 27, 34 (2001); *infra* Part IV.

28. *See infra* section IV.C.

29. *See infra* Part I.

30. *See infra* Part II.

31. *See infra* Part III.

32. *See infra* Part IV.

33. In December 2019, Apple's operating system, iOS, accounted for an estimated 55.55% of the mobile operating system market share in the United States. *See Mobile Operating System Market Share United States of America: Jan–Dec 2019*, STATCOUNTER GLOB. STATS (Dec. 2019), https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/2019 [https://perma.cc/3LMW-T9WZ]. Google's operating system, Android, accounted for an estimated 44.29%. *See id.* Together, the two operating systems accounted for an estimated 99.84% of the mobile operating system market share in the United States. *See id.*

34. *See iCloud: The Best Place for All Your Photos, Files, and More*, APPLE,

impressive capabilities provided by these platforms are possible because of developments in electronic storage and network technology, which have both undergone massive advancements in the last forty years.[35] Cloud storage platforms have fundamentally changed how people interact with technology: instead of storing a limited amount of data locally and deleting it from online storage quickly, people store vast amounts of data remotely in the cloud and keep it indefinitely.[36] This key difference has made information stored in the cloud by most Americans "detailed, encyclopedic, and effortlessly compiled."[37]

A. Technological Advances Permit Massive Cloud Data Storage

Forty years ago, data storage was expensive and had severe capacity limitations compared to today.[38] Consider the 3.5-inch floppy disk from the 1980s, which could hold 1.44 megabytes of data.[39] Compare that to the smallest storage size that Apple offers for their 2017 and newer iPhones, which is 64,000 megabytes—a 44,444-fold increase.[40] To connect with devices in the cloud, Apple now offers 5,000 megabytes of free storage and subscriptions plans with up to 2,000,000 megabytes of capacity.[41] Before Google launched their free email service in 2004, other email providers offered users about four megabytes of storage.[42] Today, Google provides 15,000 megabytes of free storage in their online storage

---

https://www.apple.com/icloud/ [https://perma.cc/S9XU-XXY2]; *Back Up or Restore Data on Your Android Device*, GOOGLE, https://support.google.com/android/answer/2819582 [https://perma.cc/6ZLR-3PJY]; *Upload Files and Folders to Google Drive*, GOOGLE, https://support.google.com/drive/answer/2424368 [https://perma.cc/JF8U-9HJR].

35. *See infra* section I.A.

36. *See infra* section I.B.

37. Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2216 (2018); *see infra* section I.B.

38. *See* R.J.T. Morris & B.J. Truskowsi, *The Evolution of Storage Systems*, 42 IBM SYS. J. 205, 205–06 (2003).

39. Steven Vaughan-Nichols, *The History of the Floppy Disk*, HEWLETT PACKARD ENTER. (Mar. 17, 2017), https://www.hpe.com/us/en/insights/articles/the-history-of-the-floppy-disk-1703.html [https://perma.cc/V8KJ-8L4W].

40. *See Identify Your iPhone Model*, APPLE (Dec. 1, 2020), https://support.apple.com/en-us/HT201296 [https://perma.cc/3HWL-UCER]. 64,000 megabytes (the smallest storage size of 2017 and newer iPhones) divided by 1.44 megabytes (the storage size of 3.5-inch floppy disks) equals a 44,444.4444-fold increase in capacity.

41. *See iCloud Storage Plans and Pricing*, APPLE (Jan. 6, 2020), https://support.apple.com/en-us/HT201238 [https://perma.cc/KTA6-XFM2] (stating that users automatically receive five gigabytes of storage for free and can purchase subscriptions for up to two terabytes of storage).

42. *See* Paul Festa, *Google to Offer Gigabyte of Free Email*, CNET (Apr. 1, 2004), http://news.cnet.com/2100-1o32-51828o5.html [https://perma.cc/WKH4-RGXA] (emphasizing that Google's new email service would "dwarf those offerings" by offering 1,000 megabytes of storage).

platform, which includes email, files, phone backups, and more.[43] Google also allows users to increase this capacity significantly with subscription plans that provide up to 30,000,000 megabytes of storage.[44]

Massive storage capacity in the cloud is only effective if users can rely seamlessly on accessing their stored information. Internet speeds have increased dramatically in the last thirty years, enabling the proliferation of online storage providers.[45] In 1994, internet-connected smartphones were unimaginable.[46] For the few that had home internet access, the fastest speed was twenty-eight kilobits per second (kbps).[47] Today, the median advertised home internet speed in the United States, including dial-up,[48] is 6,300 kbps—a 225-fold increase.[49] Cellular wireless network technologies that were invented in the early 1990s advertised download speeds of up to 200 kbps.[50] In 2010, cellular networks using more modern technology advertised average download speeds of between 5,000 and 12,000 kbps with peaks up to 50,000 kbps—up to a 250-fold increase from the second-generation network.[51]

B. Online Storage Platforms Facilitate Cloud Data Proliferation

These technological advances have led to a significant shift in user behavior. Historically, messages sent on electronic communication platforms were saved to the user's computer and deleted from remote storage in order to save space.[52] This made sense, given capacity limitations at the time. However, users today no longer need to be as concerned about space constraints; instead of deleting data to save space,

---

43. *See Storage FAQ*, GOOGLE, https://one.google.com/faq/storage [https://perma.cc/UK87-5RGG] (noting that Google offers fifteen gigabytes of free storage).

44. *See* Joe Maring, *How to Buy More Google Drive Storage*, ANDROID CENT. (Feb. 27, 2020), https://www.androidcentral.com/how-buy-more-google-drive-storage [https://perma.cc/AC2A-HFAN] (noting that Google offers paid subscriptions for up to thirty terabytes of storage).

45. *See* U.S. FED. COMMC'NS COMM'N, OBI TECHNICAL PAPER NO. 4, BROADBAND PERFORMANCE 11 (2010), https://docs.fcc.gov/public/attachments/DOC-300902A1.pdf [https://perma.cc/R85A-8J9C].

46. *See id.*

47. *Id.*

48. Dial up is a method of connecting to the internet with exclusive use of a telephone line. *Dial Up Internet Service*, VERIZON WIRELESS, https://www.verizon.com/support/residential/announcements/dial-up [https://perma.cc/TTZ7-FPGP]. Modern broadband connections are always on and use different technology than dial up. *Id.*

49. *See* U.S. FED. COMMC'NS COMM'N, *supra* note 45, at 11.

50. *Id.* at 19.

51. *See id.*

52. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 392–93 (2014).

users commonly save everything—just in case—and search for it later.[53] This new use pattern blurs the distinction between the privacy interests in real-time and stored information because it has become commonplace to store a deep record of digital communications that goes back months or even years.

The breadth of private information stored in the cloud has similarly skyrocketed. Fast internet speeds and improved storage technology allow devices to "offer a range of tools for managing detailed information about all aspects of" their users' lives.[54] Apps can be used to store passwords, watch and record videos, send messages to friends, access bank accounts, track fitness, and read the news. As the Supreme Court has recognized, this "can form a revealing montage of the user's life."[55] To preserve important data, Apple and Google provide backup services for their devices that store much of it in the cloud.[56] These services generally encrypt[57] the stored information, meaning it is somewhat protected from unauthorized access.[58] However, the platforms themselves can usually access the encrypted data because they keep the decryption key.[59] As such, cloud storage platforms generally can view much of this personal information—which can then potentially be seized and searched pursuant to a lawful order.

---

53. *See id.*

54. Riley v. California, 573 U.S. 373, 396 (2014).

55. *Id.*

56. iCloud backup includes, inter alia, app data, device settings, text messages, photos, purchase history, and the user's voicemail password. *See What Does iCloud Back Up?*, APPLE (Nov. 15, 2019), https://support.apple.com/en-us/HT207428 [https://perma.cc/5LKB-FNAL]. Android backup includes, inter alia, contacts, text messages, wi-fi network passwords, app data, and phone settings. *See Back Up or Restore Data on Your Android Device*, *supra* note 34.

57. Encrypted data cannot be viewed without using a decryption process that requires the right cryptographic private key. *See What Is Encryption? | Types of Encryption*, CLOUDFLARE, https://www.cloudflare.com/learning/ssl/what-is-encryption/ [https://perma.cc/SD8V-BKQ4] ("A cryptographic key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, [a cryptographic key] locks (encrypts) data so that only someone with the right [private] key can unlock (decrypt) it."). Using encryption prevents unauthorized parties who lack the right private key from accessing stored data. *See id.*

58. *See iCloud Security Overview*, APPLE (Nov. 18, 2019), https://support.apple.com/en-us/HT202303 [https://perma.cc/M4MS-B78W]; *Google and Android Have Your Back by Protecting Your Backups*, GOOGLE SEC. BLOG (Oct. 12, 2018), https://security.googleblog.com/2018/10/google-and-android-have-your-back-by.html [https://perma.cc/T8X2-X5VP].

59. *See iCloud Security Overview*, *supra* note 58 (noting that iCloud backup does not use end-to-end encryption for most data); *Google and Android Have Your Back by Protecting Your Backups*, *supra* note 58 (stating that the newest Android version has an end-to-end encrypted backup feature and that previous versions do not). End-to-end encryption prevents anyone besides the recipient at the other end (who has the right private key) from accessing transmitted data. *See What Is End-to-End Encryption and How Does It Work?*, PROTONMAIL (Mar. 7, 2018), https://protonmail.com/blog/what-is-end-to-end-encryption/ [https://perma.cc/RQ6F-XHGE].

Both commentators and courts have recognized that the use of modern smartphones and cloud storage platforms have led to paradigm shifts in both the depth and breadth of stored information.[60] A deep historical record is created by people constantly carrying internet-connected devices and storing functionally everything going back years. This record contains a broad array of revealing personal information about all aspects of users' lives. The Supreme Court has expressed concern when technology reveals "an individual's private interests or concerns" along with their "familial, political, professional, religious, and sexual associations."[61] The Court has also noted that some data stored in the cloud may not be shared with online storage providers in a truly voluntary manner: "Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."[62]

Although smartphones illustrate the revealing nature of data stored in the cloud, they are by no means fully responsible for the proliferation of cloud storage use. Companies offer a vast array of non-smartphone-specific cloud storage options, such as OneDrive,[63] Google Drive,[64] and Dropbox.[65] Adobe provides cloud storage for artists' photos and videos as part of their popular Creative Cloud service.[66] People even purchase home security cameras with microphones that store all of their footage in the

60. *See* Kerr, *supra* note 52, at 393; Riley v. California, 573 U.S. 373, 397 (2014); Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2218 (2018).

61. *See Riley*, 573 U.S. at 395–96 (quoting United States v. Jones, 565 U.S. 400, 415 (2012)); Kerr, *supra* note 52, at 393.

62. *See Riley*, 573 U.S. at 397. "From the user's perspective, the data that is stored on the phone and the data that is stored in the cloud and available on the phone are often indistinguishable. App data is continuously updated in order to ensure that the data is synchronized across all the users' devices [even when the user does not have the apps open]." Brief of Electronic Privacy Information Center (EPIC) et al. as Amicus Curiae Supporting Petitioner at 13, Riley v. California, 573 U.S. 373 (2014) (No. 13-132), 2014 WL 975497.

63. *See OneDrive*, MICROSOFT, https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage [https://perma.cc/GX53-6D6F] ("Save your files and photos to OneDrive and access them from any device, anywhere.").

64. *See Google Drive*, GOOGLE, https://www.google.com/intl/en/drive/ [https://perma.cc/6FP6-CTWC] ("Easy and secure access to all of your content[:] Store, share, and collaborate on files and folders from any mobile device, tablet, or computer.").

65. *See Dropbox Basic: Get a Dropbox Free Account*, DROPBOX, https://www.dropbox.com/basic [https://perma.cc/ZAU7-SMRM] ("With Dropbox Basic, it's easy to get to your files from multiple devices—computers, phones, and tablets—for free.").

66. *See Adobe Creative Cloud*, ADOBE, https://www.adobe.com/creativecloud.html [https://perma.cc/X33X-R68N] ("[T]he world's best creative apps and services so you can make anything you can imagine, wherever you're inspired."); *Find Out How Much Storage You Have*, ADOBE, https://helpx.adobe.com/creative-cloud/kb/file-storage-quota.html [https://perma.cc/XJM8-2ZU5] ("Your Creative Cloud membership comes with cloud storage.").

cloud.[67] Given the depth and breadth of data stored in the cloud, allowing unrestrained government intrusions potentially exposes even more than the most exhaustive search of a house—which is afforded strong Fourth Amendment protections against government intrusion.[68]

II. EXISTING PROTECTIONS FOR COMMUNICATIONS STORED IN THE CLOUD ARE LIMITED

The Fourth Amendment prohibits unreasonable searches and seizures and imposes specific warrant requirements to prevent a "general, exploratory rummaging in a person's belongings."[69] These protections were motivated by invasive and arbitrary general warrant searches and seizures in England and the American colonies.[70] However, existing doctrine limits the Fourth Amendment's reach in the context of data stored by third parties.[71] Against this backdrop, Congress enacted the SCA in 1986 to provide some protection, but its statutory safeguards fall below the Fourth Amendment baseline and were designed for the computer network of the past.[72] Courts have begun to recognize the privacy implications of modern technology use; in many circumstances, courts now require warrants notwithstanding lesser statutory standards.[73] Still, even when the government obtains a warrant, inconsistent approaches to the particularity requirements for electronic searches lead to widely varied

67. *See How Nest Cameras Store Your Recorded Video*, GOOGLE NEST HELP, https://support.google.com/googlenest/answer/9242083 [https://perma.cc/B8S7-HQFF] ("A Google Nest camera doesn't use memory cards to store your video on the camera. Instead, it uploads your video continuously to the cloud.").

68. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("We have said that the Fourth Amendment draws 'a firm line at the entrance to the house . . . .'" (quoting Payton v. New York, 445 U.S. 573, 590 (1980))).

69. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

70. *See infra* section II.A.

71. *See infra* section II.B.

72. *See infra* section II.C; 18 U.S.C. § 2703(d) ("A court order for disclosure . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought, [is] relevant and material to an ongoing criminal investigation."); OFF. OF LEGAL EDUC., U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 127–34 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/6SRA-WERW] (noting that § 2703(d) orders instead of warrants can compel disclosure of the contents of electronic communications in some circumstances). Professor Orin Kerr articulated a similar argument in 2004. *See* Kerr, *supra* note 15, at 1209–13. However, developments in Fourth Amendment law have led Professor Kerr to suggest that the content of communications such as email may receive constitutional protection. *See* Kerr, *supra* note 52, at 399–400.

73. *See infra* section II.C.

levels of judicial oversight.[74]

A. Foundational Fourth Amendment Principles

The purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[75] This has been clear since its adoption—its protections were motivated by arbitrary and unreasonable privacy invasions by the British.[76] In England during the late 1400s and early 1500s, the British used "general warrants" to conduct unjustified searches "wherever it shall please them."[77] The invasiveness of searches worsened in the early 1600s with the creation of "writs of assistance" that expanded the scope of general-warrant searches.[78] These searches were "abhorred by the [American] colonists."[79] During the first judicial challenge to the writs in the American colonies, the lawyer arguing against the practice gave an influential oratory that, according to John Adams, "breathed into this nation the breath of life."[80] Although the challenge failed,[81] the Supreme Court has characterized the lawyer's oratory "as perhaps the most prominent event" inaugurating the resistance of the colonies.[82] The Court has also stated it is "familiar history" that such searches and seizures "were the immediate evils that motivated the framing and adoption of the Fourth Amendment."[83]

To prevent unbridled authority in conducting invasive intrusions, the Fourth Amendment safeguards "persons, houses, papers, and effects, against unreasonable searches and seizures" by the government.[84] Under *Katz v. United States*[85] and its progeny, government action is a search under the Fourth Amendment if it violates a person's "reasonable

---

74. *See infra* section II.D.

75. Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967)).

76. JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT 20–21 (1966); Stanford v. Texas, 379 U.S. 476, 481–82 (1965).

77. LANDYNSKI, *supra* note 76, at 21 (citing 1 A TRANSCRIPT OF THE REGISTERS OF THE COMPANY OF STATIONERS OF LONDON, 1554–1640, A.D., at xxxi (Edward Arber ed., 1875)).

78. *Id.* at 22–23.

79. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

80. NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 59 (1970).

81. *Id.* at 63.

82. Stanford v. Texas, 379 U.S. 476, 481 (1965).

83. Payton v. New York, 445 U.S. 573, 583 (1980).

84. U.S. CONST. amend. IV.

85. 389 U.S. 347 (1967).

expectation of privacy."[86] This standard has two discrete components: (1) a person must have "exhibited an actual (subjective) expectation of privacy," and (2) that expectation must be "one that society is prepared to recognize as 'reasonable.'"[87] If either component is not satisfied, the Fourth Amendment does not apply.[88] *Katz* explicitly rejected the prevailing interpretation that only property interests control; instead, the Court emphatically stated that "the Fourth Amendment protects people, not places."[89]

Once government action implicates the Fourth Amendment, it is generally unreasonable in the absence of a valid warrant.[90] The Fourth Amendment permits warrants to be issued only "upon probable cause" and requires that they "particularly describ[e] the place to be searched, and the . . . things to be seized."[91] Probable cause is a "fluid concept"[92] that is satisfied when there is a reasonable basis to believe that an individual has committed a crime—a determination that is highly dependent on specific facts and circumstances.[93] The dual "place" and "things" requirements for particularity are closely related and fact-dependent; there must be probable cause that (1) the items will be found in the specified place, and (2) the specifically described items are connected with a crime.[94] The warrant's description must enable an officer to reasonably identify the items that are authorized to be seized and permit an issuing magistrate to determine whether the entire seizure is supported by probable cause.[95]

---

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

87. Smith v. Maryland, 442 U.S. 735, 740 (1978) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

88. *See* 1 WAYNE R. LAFAVE, SEARCH & SEIZURE § 2.1(b) (6th ed. 2020).

89. *Katz*, 389 U.S. at 351.

90. Riley v. California, 573 U.S. 373, 382 (2014) ("Our cases have determined that '[w]here a [Fourth Amendment] search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant.'" (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995))).

91. U.S. CONST. amend. IV.

92. Illinois v. Gates, 462 U.S. 213, 232 (1983).

93. United States v. Davis, 458 F.2d 819, 821 (D.C. Cir. 1972).

94. *See* U.S. CONST. amend. IV; United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986); State v. Perrone, 119 Wash. 2d 538, 548–49, 834 P.2d 611, 616–17 (1992); 2 LAFAVE, *supra* note 88, § 4.6(a). The specificity required for particularization depends greatly on individual facts and circumstances, including the crime and the items involved; often, "the sufficiency of a description of items to be seized . . . cannot be made by reference to earlier decisions passing upon precisely the same type of description." *Id.* § 4.6(a). Instead, the description in each case must be evaluated in terms of the purposes that underlie the particularization requirement. *Id.* Warrants should describe the items to be seized as particularly as possible but use of generic categories does not necessarily invalidate a warrant if it is not possible to use a more precise description. *See Spilotro*, 800 F.2d at 963.

95. *See Spilotro*, 800 F.2d at 963; 2 LAFAVE, *supra* note 88, § 4.6(a).

The Supreme Court has identified two distinct constitutional justifications for these requirements.[96] First, there should be "a careful prior determination of necessity" because "any intrusion in the way of search or seizure is an evil."[97] Second, "searches deemed necessary should be as limited as possible" to prevent "a general, exploratory rummaging in a person's belongings."[98] The authorization to search and seize should be limited to the specific areas and things for which there is probable cause so that the government intrusion is carefully tailored to its justifications.[99]

B. The Third-Party Doctrine Restricts the Fourth Amendment's Reach

Various caveats have emerged over time to these bedrock Fourth Amendment principles; among them—and crucial for data stored in the cloud—is the third party doctrine.[100] Its roots can be traced to *Katz*, which clarified that "[w]hat a person knowingly exposes to the public, even in [their] own home or office, is not a subject of Fourth Amendment protection."[101] In *United States v. Miller*,[102] the Supreme Court relied in part on this language to hold that the Fourth Amendment does not apply to bank records, such as checks and deposit slips, because they were business records that were voluntarily disclosed to third parties.[103] Three years later, in *Smith v. Maryland*,[104] the Court adopted similar reasoning to find that pen registers, which were devices that recorded what phone numbers were dialed but not conversations, did not implicate the Fourth Amendment and therefore did not require a warrant.[105]

In the past, the Supreme Court also justified the third-party doctrine by

---

96. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

97. *Id.* (emphasis omitted).

98. *Id.*

99. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

100. *See infra* notes 103–115 and accompanying text. Other caveats to these bedrock principles include the good faith exception, open fields, exigent circumstances, and community caretaking. *See* United States v. Leon, 468 U.S. 897, 922–23 (1984) (good faith exception); 1 LAFAVE, *supra* note 88, § 1.3(a) (good faith exception); *id.* § 2.4(a) (open fields); Oliver v. United States, 466 U.S. 170, 181–84 (1984) (open fields); Welsh v. Wisconsin, 466 U.S. 740, 749–53 (1984) (exigent circumstances); 3 LAFAVE, *supra* note 88, § 6.1(f) (exigent circumstances); *id.* § 6.6(a) (community caretaking); Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (community caretaking).

101. Katz v. United States, 389 U.S. 347, 351 (1967). But importantly, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351–52.

102. 425 U.S. 435 (1976).

103. *Id.* at 442.

104. 442 U.S. 735 (1979).

105. *Id.* at 740–46. Phone numbers are voluntarily disclosed to third parties, but the conversations are not. *See id.*

reasoning that individuals assume the risk that another person might reveal their affairs to the government when they reveal their affairs to that third party.[106] But subsequent developments in Fourth Amendment doctrine have clarified that the act of sharing is not itself determinative and people can still retain a reasonable expectation of privacy in data shared with a third party.[107]

Courts, policymakers, and commentors analyzing *Miller* and *Smith* often identify a distinction between content and non-content.[108] Content is information that conveys the substance or meaning of a communication, whereas non-content is information that does not.[109] This distinction can be traced to postal mail letters, where the content of the letter itself is entitled to Fourth Amendment protection but the non-content addressing information on the envelope is not.[110] Similarly, the content of a phone conversation is entitled to Fourth Amendment protection, but the phone number that is dialed (and revealed to third parties) is not.[111] This principle can also apply to the cloud, with a distinction between the content of private communications and the non-content addressing or subscriber information.

The United States Department of Justice (DOJ) accepted the distinction between content and non-content for data stored in the cloud but took the position that a warrant is not required to obtain either content or non-content.[112] With regard to non-content, such as subscriber information and transactions records, the DOJ suggested that the third-party doctrine precludes any reasonable expectation of privacy at all.[113] With regard to content, for which users may have a reasonable expectation of privacy, the DOJ suggested that a "reasonable" subpoena may be used to compel production,[114] which would be subject to a lower standard than a

106. *Id.* at 740–44.

107. *See* Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2219 (2018); *infra* section III.B.

108. *See infra* notes 131–136 and accompanying text; *infra* section II.C; Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009) ("The content/noncontent distinction remains important in the constitutional and statutory law governing the inspection of private communications, even as new technologies have dramatically altered the nature of communication itself.").

109. *See* 18 U.S.C. § 2510(8); Tokson, *supra* note 108, at 2112.

110. *See Ex parte* Jackson, 96 U.S. 727, 733 (1878); Tokson, *supra* note 108, at 2112.

111. *Smith*, 442 U.S. at 741–46.

112. OFF. OF LEGAL EDUC., *supra* note 72, at 144–47 (stating that it is "well established that a customer or subscriber has no reasonable expectation of privacy in [their non-content] subscriber information or transactional records" but "whether a user has a reasonable expectation of privacy in the contents of communications . . . will depend on the facts and circumstances").

113. *Id.* at 144.

114. *Id.* at 145. Subpoenas are used by a variety of government actors to compel production of

warrant.[115] The DOJ's view has recently been called into question, as discussed further below,[116] but it parallels the statutory framework that protects information stored in the cloud today.

C. Limited Statutory Protection from the Stored Communications Act

In 1986, against the backdrop of the third-party doctrine's limitations on constitutional protections, Congress enacted the SCA as a statutory framework to safeguard electronic communications stored by third-parties.[117] The SCA incorporated computer network use patterns at the time.[118] Back then, online services had two main purposes.[119] One purpose was email, which was generally stored online only until it was delivered to the user's local machine.[120] The other purpose was outsourcing computing tasks, such as storing files remotely and processing large amounts of data.[121] To provide protection for these specific purposes, the SCA regulates electronic communication services (such as email) and remote computing services (such as remote file storage and data processing).[122] Despite that technology use patterns today are fundamentally different than when the SCA was enacted over thirty years ago, this framework still applies to stored electronic communications.

The SCA incorporated the distinction between content and non-content, defining content as "any information concerning the substance,

---

documents, including business and tax records. *See* 2 LAFAVE, *supra* note 88, § 4.13. The recipient has an opportunity to challenge, or quash, the subpoena before producing the requested materials. *Id.* Protection against unreasonable subpoenas traditionally flows from the Fifth Amendment, but the Fourth Amendment is also implicated. *Id.*

115. *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208–09 (1945); See v. City of Seattle, 387 U.S. 541, 544 (1967) (noting that a subpoena must be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome"); 2 LAFAVE, *supra* note 88, § 4.13(a). Unlike warrants, which are used to prove a pending charge, subpoenas are primarily used to discover evidence and ascertain the extent of wrongdoing to make a charge. *See* Subpoena Duces Tecum v. Bailey, 228 F.3d 341, 247 (4th Cir. 2000).

116. *See infra* notes 131–136 and accompanying text.

117. 18 U.S.C. §§ 2701–13.

118. *See* Kerr, *supra* note 15, at 1213–14.

119. *See* S. REP. NO. 99-541, at 2–3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556–57.

120. *See* H.R. REP. NO. 99-647, at 22 (1986).

121. *See* S. REP. NO. 99-541, at 3.

122. *See* 18 U.S.C. § 2510(15) (electronic communication service defined as any service which provides its users the ability to send or receive wire or electronic communications); *id.* § 2510(17) (electronic storage is defined as any temporary or intermediate storage of such a communication or backup thereof); *id.* § 2711(2) (remote computing service defined as "the provision to the public of computer storage or processing services by means of an electronic communications system"); *id.* § 2510(14) (defining electronic communications system).

purport, or meaning of that communication."[123] By its terms, the SCA permits the government to compel disclosure of non-content and almost all content held by cloud storage providers with a court order under 18 U.S.C. § 2703(d) instead of a warrant.[124] To obtain a 2703(d) order, the government must present "specific and articulable facts showing that there are reasonable grounds to believe that the [information is] relevant and material to an ongoing criminal investigation."[125] This is a lower standard than probable cause and does not require any showing of wrongdoing by the user. The only type of information that requires a warrant supported by probable cause is unopened email that has been in storage for 180 days or less.[126] In a concession to the reality of modern technology use, some courts have construed the warrant requirement to extend also to opened email in storage for 180 days or less.[127]

The protections afforded by the SCA were understandable at the time it was enacted, considering the newly emerging third-party doctrine combined with slow network speeds and the lack of electronic storage capacity in the 1980s.[128] However, due to seismic technological shifts, some justifications for its distinctions may no longer hold.[129] For example, the distinction between unopened email stored less than 180 days (which requires a warrant under the SCA) and other remotely stored data (which does not) was only salient because, at the time, email was not stored by online providers for long periods of time.[130]

Some courts have begun to recognize the implications of these technological shifts on Fourth Amendment doctrine and accordingly have required a warrant to access private communications. For example, in *United States v. Warshak*,[131] the United States Court of Appeals for the Sixth Circuit found that users have a reasonable expectation of privacy in the content of emails stored by service providers.[132] The court analogized

123. 18 U.S.C. § 2510(8); *id.* § 2711(1) ("[T]he terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section . . . .").

124. *See* 18 U.S.C. § 2703(d); *id.* § 2703(a)–(b) (compelled disclosure of content); *id.* § 2703(c) (compelled disclosure of non-content, including subscriber information, telephone connection records, and payment information); Kerr, *supra* note 15, at 1222–24.

125. 18 U.S.C. § 2703(d).

126. *Id.* § 2703(a).

127. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2006) ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage.").

128. *See* United States v. Miller, 425 U.S. 435, 442–46 (1976); Smith v. Maryland, 442 U.S. 735, 741–46 (1979); Kerr, *supra* note 15, at 1213–18; *supra* Part I.

129. *See supra* Part I.

130. *See supra* Part I.

131. 631 F.3d 266 (6th Cir. 2010).

132. *Id.* at 285–86.

email to postal mail, where the letter is content—entitled to full Fourth Amendment protection—and the addressing information is non-content that is not protected.[133] "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[134] Therefore, "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[135] Other courts have adopted this approach,[136] and many cloud storage providers already require a warrant to obtain private communications.[137] However, the Supreme Court has not yet settled the matter.

D. Inconsistent Approaches to the Warrant Particularity Requirement

Even when the government uses a warrant to obtain private communications stored in the cloud, courts take a variety of inconsistent approaches to the warrant particularity requirement.[138] In the context of physical electronic storage media, such as hard drives and USB sticks, sifting through large amounts of data at crime scenes to find information responsive[139] to a warrant is fraught with challenges. According to DOJ, "it will be infeasible in almost every case" to search physical electronic media at the scene because evidence may be mislabeled, hidden, or otherwise "difficult to locate and retrieve without the appropriate tools and time."[140] Courts also recognize that searches and seizures of physical electronic media pose significant challenges because data are interspersed

133. *Id.*

134. *Id.*

135. *Id.* at 288.

136. *See, e.g.*, *In re* Applications for Search Warrants for Info. Associated with Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider."); United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (reasonable expectation of privacy in email).

137. *See Legal Process Guidelines: Government & Law Enforcement Within the United States*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/RY8S-V5BC]; *How Google Handles Government Requests for User Information*, GOOGLE, https://policies.google.com/terms/information-requests [https://perma.cc/WF7X-X75Y]; *About Our Practices and Your Data*, MICROSOFT, https://blogs.microsoft.com/datalaw/our-practices [https://perma.cc/9ZAV-UVYN].

138. *See* FED. R. CRIM. P. 41(e)(2); *infra* notes 147–163 and accompanying text.

139. Responsive information corresponds with the particularized terms of the warrant; conversely, items that are outside the scope of the warrant's terms are nonresponsive. *See* United States v. Ganias, 824 F.3d 199, 210 n.23 (2d Cir. 2016); United States v. Aboshady, 297 F. Supp. 3d 232, 236 (D. Mass. 2018).

140. OFF. OF LEGAL EDUC., *supra* note 72, at 76–77.

throughout, making extraction and segregation of responsive data from nonresponsive data potentially impossible without retaining the media itself (or an exact copy).[141] Even attempting to search physical electronic media at the scene risks damaging evidence because simply using the media might alter the stored data.[142] Furthermore, seizures of physical electronic media may be necessary for the government to establish the authenticity and integrity of evidence at trial, and for the defendant to challenge evidence through an independent forensic analysis.[143]

To address these challenges, Federal Rule of Criminal Procedure 41(e)(2) authorizes a two-step process for searches and seizures of electronically stored data.[144] The process begins with an initial broader seizure of the physical electronic storage media, or the copying of the data stored on it.[145] Then, once the media is seized, the government can subsequently search it at a later date to identify information that is responsive to the warrant's narrower subject matter restrictions.[146]

United States v. Pinto-Thomaz[147] illustrates a deferential approach to this Rule applied to seizures of private communications stored in the cloud. The warrant issued in *Pinto-Thomaz* required production of data stored in an Apple iCloud account that was associated with Pinto-Thomaz's email address.[148] It demanded that Apple produce messages, images, videos, files, documents, address book information, subscriber and payment information, transaction records, Find My iPhone device location connection logs, service information, along with "[a]ll records and other information stored by the . . . user."[149] Instead of imposing specific restrictions on the initial seizure from the service provider, the warrant allowed the government to look through this vast quantity of seized data to identify what might fall under the warrant's more narrowly

141. *See Ganias*, 824 F.3d at 212–14.

142. *See id.* at 212 n.28; OFF. OF LEGAL EDUC., *supra* note 72, at 77–78. Computers continually read from and write to the hard disk, which changes some of the information recorded there. OFF. OF LEGAL EDUC., *supra* note 72, at 77–78. Furthermore, if a device is connected to the internet, "someone at a remote location might be able to access the computer and delete data while investigators are examining it on-site." *Id.* at 77–78.

143. *See Ganias*, 824 F.3d at 215–16. *But see id.* at 215 n.33 ("We do not suggest that authentication of evidence from computerized records is impossible absent retention of an entire hard drive or mirror.").

144. FED. R. CRIM. P. 41(e)(2).

145. *Id.*

146. *Id.*

147. 352 F. Supp. 3d 287 (S.D.N.Y. 2018).

148. Government's Memorandum of Law in Opposition to Defendants' Pretrial Motions at Ex. D, *Pinto-Thomaz*, 352 F. Supp. 3d 287 (No. S2 18-Cr.-579 (JSR)).

149. *Id.*

particularized subject-matter limitations.[150]

The warrant included an explicit time limit on how old the messages in the initial seizure could be but it did not specify such a limit for any other categories of requested data.[151] Even with these open-ended parameters, the *Pinto-Thomaz* court found that the warrant was not facially overbroad because "a temporal limitation is not an absolute necessity."[152] Notwithstanding the invasive nature of the initial seizure, the court held that the more narrowly particularized subject matter limitations on the subsequent search effectively limited the time frame concerned.[153] However, those limitations were not clear to the FBI agent who searched the materials, leading the agent to review materials that fell outside the warrant's limitations on the subsequent search.[154]

The government regularly applies for warrants that demand a vast array of information from cloud storage providers. For example, a narcotics investigator requested the authority to seize all content[155] from an Apple iCloud account.[156] According to the agent's affidavit, it was necessary to copy the entire contents of the account to minimize interference with the cloud storage provider's business activities, protect privacy of other users, and "effectively pursue this investigation."[157] Other examples include a firearms trafficking investigator and a postal inspector who both requested the authority to seize, among other things, "[t]he contents of all files and other records stored on iCloud."[158] While each application also contained

---

150. *See* United States v. Pinto-Thomaz, 357 F. Supp. 3d 324, 329–31 (S.D.N.Y. 2019).

151. Government's Memorandum of Law in Opposition to Defendants' Pretrial Motions, *supra* note 148, at Ex. D. Perhaps surprisingly, not even "[a]ll records and other information stored by the Subject Account's user" had an explicit time limitation. *Id.*

152. *Pinto-Thomaz*, 352 F. Supp. 3d at 306 (quoting United States v. Hernandez, No. 09-cr-625, 2010 U.S. Dist. LEXIS 719, at *37 (S.D.N.Y. Jan. 6, 2010)).

153. *Id.* at 306–07.

154. *Pinto-Thomaz*, 357 F. Supp. 3d at 330. Even after these violations, the court found "no ground for imposing the 'extreme remedy' of blanket suppression" because the agent did not "grossly exceed" the warrant's terms, which "generally authorized widespread seizure of a number of broadly defined categories of evidence." *Id.* at 331.

155. The agent did not appear to be making a distinction between content and non-content. *See* Application for a Search Warrant at Attach. B, *In re* the Search of Apple, Inc., No. 19MJ5303 (S.D. Cal. Nov. 27, 2019) [hereinafter Search Warrant Application for cmdlc92@icloud.com] (requesting subscriber information, billing records, electronic mail, files, cloud storage, location information, and more).

156. *Id.*

157. *Id.* at 16. The agent did not provide any citations for these assertions. *See id.*

158. Application for a Search Warrant at Attach. B, *In re* the Search of Info. Associated with the Apple ID & iCloud Account grindfamily1@gmail.com that Is Stored at Premises Controlled by Apple Inc., No. 19-968M(NJ) (E.D. Wis. Feb. 20, 2020) [hereinafter Search Warrant Application for grindfamily1@gmail.com] (firearms trafficking investigator); Application for a Search Warrant at 24,

an enumerated list of items to obtain, the provisions above seem to make such a list somewhat superfluous because the scope of the requested seizure was, in effect, all information associated with the cloud storage provider accounts.[159]

Not all courts endorse such a deferential approach to the particularization of the initial seizure. For example, the United States Court of Appeals for the Eleventh Circuit suggested that warrants for broad categories of data might be invalid under the Fourth Amendment because "[t]hey require[] disclosure to the government of virtually every kind of data that could be found in a social media account."[160] As such, they should have been limited to communications between specific persons and during specific periods.[161] Some courts have gone even further and suggested that cloud storage providers filter the requested information using specifically designated search parameters before providing it to the government.[162] However, other courts have rejected this approach, in part because incidental exposure to some nonresponsive information is unavoidable even with searches of physical items.[163] This variation in approach by jurisdiction, with many adopting a deferential approach, fails to provide consistent protection against unreasonable searches and seizures of private communications stored in the cloud.

In re the Search of Info. Associated with peter_burno@icloud.com that Is Stored at Premises Controlled by Apple, Inc, No. 3:19-MJ-00578-MMS (D. Alaska Nov. 27, 2019) [hereinafter Search Warrant Application for peter_burno@icloud.com] (postal inspector).

159. *See* Search Warrant Application for grindfamily1@gmail.com, *supra* note 158, at Attach. B; Search Warrant Application for peter_burno@icloud.com, *supra* note 158, at 23–26; Search Warrant Application for cmdlc92@icloud.com, *supra* note 155, at Attach. B.

160. United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017).

161. *Id.* However, regardless of any potential Fourth Amendment violation, the court found that the obtained evidence should not be excluded due to the good-faith exception. *Id.*

162. *See In re* the Search of Info. Associated with [redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 8–9 (D.D.C. 2014); *In re* the Search of Info. Associated with [redacted]@mac.com That is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 153–55 (D.D.C.), *vacated*, 13 F. Supp. 3d 157, 168 (D.D.C. 2014).

163. *See In re* the Search of Info. Associated with [redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 166 (D.D.C. 2014); United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) ("The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching."); United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010) ("Nor does the Fourth Amendment require the executing authorities to delegate a pre-screening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.").

III. PAST UNREASONABLE SEIZURES ENABLED BY TECHNOLOGICAL ADVANCEMENT

The Supreme Court has long recognized that technology has the potential to increase the government's power to conduct invasive and unjustified seizures.[164] When confronted with such technology, the Court has expanded Fourth Amendment protection to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[165] One of those moments occurred when the Court confronted invasive real-time telephone wiretapping, recognizing its similarity to general warrants of the past.[166] More recently, the Court has reevaluated existing Fourth Amendment doctrine to maintain protection for data that, due to its depth and breadth, has the potential to be highly revealing.[167]

A. Berger*: Real-Time Wiretapping Recognized as Invasive*

In 1967, the Supreme Court confronted real-time eavesdropping through wiretapping, a then-modern technology that could enable highly invasive searches and seizures of private communications.[168] At the time, a New York statute authorized judicial wiretap orders that were founded on a "reasonable ground to believe that evidence of a crime may be thus obtained," not probable cause.[169] The statute also required that orders state their duration, with a maximum of two months (unless extended), the telephone line (if relevant), and a particular description of "the person or persons whose communications, conversations or discussions are to be overheard or recorded and the purpose thereof."[170] An order could be extended if it was "in the public interest"—a vague standard that did not clearly require a new showing of probable cause.[171]

After examining the invasiveness of the seizure, the Court first emphasized that a warrant based on probable cause is required under the Fourth Amendment.[172] Although some New York cases suggested that the

---

164. *See* Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2214 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

165. *Id.*

166. *See* Berger v. New York, 388 U.S. 41, 58 (1967).

167. *See* Riley v. California, 573 U.S. 373, 403 (2014) (cell phones incident to arrest); *Carpenter*, 138 S. Ct. at 2217 (cell site location information).

168. *Berger*, 388 U.S. at 46–47.

169. *Id.* at 43 n.1.

170. *Id.*

171. *Id.* at 59.

172. *Id.* at 55 (quoting U.S. CONST. amend. IV).

statute's "reasonable ground" requirement was equivalent, the Court decided it "need not pursue the question further" because "the statute is deficient on its face in other respects."[173]

Specifically, the Court found that the statute did not satisfy the Fourth Amendment's warrant particularization requirement.[174] While it did require identification of the "persons whose communications . . . are to be overheard," the statute did not require particularity as to the specific crime that was committed, the specific place to be searched, or the specific communications to be seized.[175] As such, the statute lacked the necessary "precise and discriminate requirements" and instead authorized "indiscriminate use" of wiretapping.[176] The Court also found that "[t]he need for particularity and evidence of reliability in the showing required . . . is especially great in the case of eavesdropping" because "[b]y its very nature eavesdropping involves an intrusion on privacy that is broad in scope."[177] The New York statute also impermissibly sanctioned "long and continuous" eavesdropping that allowed officers to seize communications "indiscriminately and without regard to their connection with the crime under investigation."[178] The Court found that the statute was unconstitutional because it authorized invasive general-warrant searches that the Fourth Amendment was specifically intended to prevent.[179]

Just one year after *Berger*, Congress enacted Title III to regulate real-time wiretapping.[180] This new statute was designed to meet and build on *Berger*'s requirements.[181] Along with an explicit warrant requirement, Title III also mandates minimization requirements,[182] notice to targets,

---

173. *Id.*

174. *Id.*

175. *Id.* at 58–59.

176. *Id.* at 58.

177. *Id.* at 56.

178. *Id.* at 59. The Court also required a showing of "present probable cause" instead of only relying on the original grounds in the initial order. *Id.*

179. *Id.* at 58.

180. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 212 (codified as amended in scattered sections of 18 U.S.C.); *see also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 21–23 (2004). "Commentators use either 'Title III' or the 'Wiretap Act' to refer to the law." Freiwald, *supra*, at 13 n.22.

181. Freiwald, *supra* note 180, at 24 ("When Congress passed the Wiretap Act in 1968, it benefited from the Supreme Court's recent guidance.").

182. Title III mandates that every wiretap order and extension "contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this

extensive involvement of a judicial officer, and even prohibits wiretapping until conventional techniques have failed.[183] At least one commentator has called a Title III judicial order for wiretapping a "super-warrant."[184] The statutory provisions in Title III provide even stronger privacy protections than those required in *Berger* and demonstrate that legislation can create an effective statutory framework that exceeds a constitutional baseline.

B. Riley *and* Carpenter*: Highly Revealing Nature of Stored Data Leads to Revised Fourth Amendment Doctrines*

The Supreme Court has recently re-examined existing Fourth Amendment doctrines in the context of highly revealing searches and seizures but has not yet considered the Fourth Amendment protections for private communications stored in the cloud. First, in *Riley v. California*,[185] the Court narrowed the authority for officers to search the contents of cell phones seized incident to a lawful arrest. The Court explicitly rejected the argument that searching data stored directly on a cell phone is indistinguishable from searches of physical containers.[186] Instead, the Court found that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[187] Given their immense storage capacity and propensity to collect many distinct types of information, cell phones store a deep record of users' everyday lives.[188] Furthermore, the breadth of data collected—including location information, messages, a plethora of apps, browsing data, and search history—"can form a revealing montage of the user's life."[189] These factors led the Court to require a warrant prior to searching a cell phone, even incident to arrest.[190]

Four years later, in *Carpenter v. United States*,[191] the Court confronted

---

chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception." 18 U.S.C. § 2518(5).

183. Omnibus Crime Control and Safe Streets Act of 1968 § 802; Freiwald, *supra* note 180, at 25.

184. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 630 (2003).

185. 573 U.S. 373 (2014).

186. *Id.* at 392–93.

187. *Id.* at 393.

188. *Id.* at 393–94.

189. *Id.* at 396.

190. *Id.* at 401.

191. 585 U.S. __, 138 S. Ct. 2206 (2018).

the warrantless acquisition of cell phone users' stored location information under the SCA.[192] Cell phones connect to towers near their users for communication, and cellular providers store these time-stamped records of their customers' approximate locations over time; these records are called cell-site location information (CSLI).[193] Although wireless providers collect and store these records for their own business purposes,[194] CSLI also "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[195] Furthermore, because cell phones are "indispensable to participation in modern society" and "[v]irtually any activity on the phone generates CSLI," users do not "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements."[196]

Even though CSLI arguably consists of business records held by a third party, the Court declined to extend the third-party doctrine to the collection of CSLI and instead required a warrant.[197] In *Carpenter*, the Court made it clear that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[198] The Court also noted that it "has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy."[199] Taken together, *Riley* and *Carpenter* suggest that, when technology enables the depth and breadth of stored data to become sufficiently "detailed, encyclopedic, and effortlessly compiled,"[200] courts should evaluate such impacts to protect users' reasonable expectation of privacy.

IV. PROTECTING A REASONABLE EXPECTATION OF PRIVACY IN THE CLOUD

It is paramount to recognize when technology enables the government to conduct searches and seizures that are akin to general warrant searches

192. *Id.* at 2212–13.

193. *See id.* at 2211–12.

194. *Id.* at 2212.

195. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

196. *Id.* at 2220 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

197. *Id.* Although the Court required a warrant for seven days of CSLI, it left open the possibility that accessing a more "limited period" of CSLI might survive Fourth Amendment scrutiny. *Id.* at 2217 n.3.

198. *Id.* at 2217.

199. *Id.* at 2221.

200. *See id.* at 2216.

the framers intended to prohibit, especially in light of the purpose of the Fourth Amendment—to prevent officers from having unbridled discretion to perform unreasonable government intrusions. As with real-time wiretapping in *Berger*, seizing private communications stored in the cloud without sufficient safeguards is akin to an invasive general warrant search. To provide sufficient safeguards, courts should consider the fundamental privacy implications of seizing what is often years' worth of revealing private communications stored in the cloud and adopt Fourth Amendment doctrine to prevent such invasive and unreasonable seizures.

A. Seizures of Private Communications in the Cloud Should Require a Warrant and Probable Cause

A warrant should be required to obtain private communications stored in the cloud due to the highly invasive nature of such seizures. Users often store years of wide-ranging private communications in the cloud.[201] Seizures of such communications "form a revealing montage of the user's life,"[202] and cloud storage platforms have become functionally "indispensable to participation in modern society,"[203] akin to smartphones. When users store intimate information in the cloud, including video and audio recordings from inside their homes,[204] it seems clear they possess a subjective expectation of privacy in those stored communications. Additionally, given the ubiquity of online storage platforms today and their intimate interdependence with modern devices,[205] society appears to recognize this expectation as reasonable.[206]

Berger supports these conclusions—it made clear that obtaining functionally every communication a person had over an extended period of time required a warrant supported by probable cause.[207] Although the threat then was real-time wiretapping, the government today can obtain years' worth of messages that a user sends and receives, location history, photos, videos, phone backups, and more from the cloud.[208] Furthermore, the Court underscored in *Carpenter* that users can retain a reasonable

201. *See supra* section I.B.

202. Riley v. California, 573 U.S. 373, 396 (2014); *see also supra* section I.B.

203. *Carpenter*, 138 S. Ct. at 2220; *see also supra* section I.B.

204. *See supra* section I.B.

205. *See supra* section I.B.

206. Prominent cloud storage providers like Apple, Google, and Microsoft seem to agree that the Fourth Amendment requires the government to obtain a warrant for private communications stored in the cloud. *See supra* notes 131–137 and accompanying text (warrant based on probable cause required to obtain user content stored in the cloud).

207. *See* Berger v. New York, 388 U.S. 41, 55–59 (1967); *supra* section III.A.

208. *See supra* notes 122–163 and accompanying text; *supra* section I.B.

expectation of privacy in data stored with a third party if that data are sufficiently revealing and the technology is indispensable.[209] Accordingly, courts should recognize the necessity for a warrant requirement to obtain private communications stored in the cloud and invalidate the SCA to the extent that it allows access to such data without a warrant and with a lower standard than probable cause.

B. Berger-*like Enhanced Particularity Requirements Should Apply*

Given the inconsistent approaches to the particularity requirement for electronic searches and seizures, a warrant is necessary but not sufficient to safeguard private communications stored in the cloud. Courts should recognize, as in *Berger*, that "[t]he need for particularity and evidence of reliability in the showing required . . . is especially great" for communications held in the cloud because such seizures involve "an intrusion on privacy that is broad in scope."[210] Furthermore, as the United States Court of Appeals for the Second Circuit noted, it is crucial to engage with the technological specifics.[211] With these considerations in mind, courts should balance users' privacy interests with officers' legitimate need to find evidence of wrongdoing—as long as there is probable cause.

Under this approach, a warrant that authorizes the initial seizure of all information stored by the user[212] of a cloud storage provider account would by facially invalid due to the lack of particularization. Instead, the government should be required to particularize the warrant to the extent it can do so without requiring the platform to comb through the content of users' private communications. A government mandate that forces cloud storage providers to build highly specialized systems and hire staff to comb through the content of user data would have privacy implications for other users and interfere with the provider's business activities.[213]

Temporal limitations, such as "all messages sent and received between these dates," should be required because they do not require any knowledge of the content of communications. In addition, warrants should particularly describe the type of content requested and show the probable cause that supports such a request. Communications stored in the cloud

---

209. Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2217 (2018); *see also supra* notes 192–200 and accompanying text.

210. *See Berger*, 388 U.S. at 56; *supra* section I.B.

211. United States v. Ganias, 824 F.3d 199, 217 (2d Cir. 2016).

212. *See supra* notes 147–154 and accompanying text.

213. *See supra* notes 155–157 and accompanying text; Bihter Ozedirne, Note, *Fourth Amendment Particularity in the Cloud*, 33 BERKELEY TECH. L.J. 1223, 1239–40 (2018).

can take a wide variety of forms, including text messages, email, photos, videos, files, browsing history, phone backups, and more.[214] If the government has information that suggests two individuals used a cloud storage account to contact each other in furtherance of a crime during a specified time period, that would support probable cause for the government to seize any messages between those individuals during the specified period. But, standing alone, that information should not be sufficient to support probable cause permitting the government to also seize photos or browsing history from that same period.

Particularization of this sort is possible because the government can request specific categories of information from the cloud storage provider.[215] This makes searches in the cloud materially different from searches of physical electronic storage media: there is no scene of the crime, so to speak, and no need for the government to conduct a forensic analysis of the raw storage media to discover evidence. Furthermore, probable cause can be more specifically associated with the categories of data that are initially seized. Thus, the traditional justifications for allowing unrestrained initial seizures of physical electronic storage media[216] apply with less force, and the intermediary role of the provider should generally permit reasonable limits on the initial seizure.

C. Compatible Statutory Protections Should Provide Future Comprehensive Framework

The proposed safeguards in this Comment are designed as a constitutional baseline, not a comprehensive regulatory framework. Like with *Berger* and Title III, Congress should build off this constitutional approach and enact revised statutory protections.[217] Ideally, these protections would go beyond the baseline to protect users' reasonable expectation of privacy while still addressing the government's legitimate interest in investigating wrongdoing. For example, akin to Title III, Congress could permit the acquisition of private communications stored in the cloud only for a specific list of enumerated offenses, require that traditional investigatory techniques be tried first and fail, or require notice

214. *See supra* section I.B.

215. *See Legal Process Guidelines*, *supra* note 137 (specifying twenty-three different categories of available information and asking that government requests "be as narrow and specific as possible"); *Requests for User Information FAQs*, GOOGLE, https://support.google.com/transparencyreport/answer/9713961 [https://perma.cc/63MG-77D5] (specifying a variety of types of available information depending on the relevant Google services).

216. *See supra* notes 139–143 and accompanying text.

217. *See* Freiwald, *supra* note 180, at 24–26.

to targets of the investigation.[218] Congress could also mandate specific minimization requirements, such as a presumptive maximum temporal limit for the acquisition of private communications that could only be overcome with a heightened showing in specified circumstances. Regardless, any statutory safeguards should mandate the extensive involvement of the court in the entire process.

CONCLUSION

Although users store a vast amount of private information in the cloud, such information currently only receives limited protection from unreasonable government intrusions. Existing statutes allow the government to obtain many private communications without a warrant and using a lower standard than the constitutional baseline of probable cause. Even with a warrant, inconsistent approaches to particularization fail to provide consistent protection against unreasonable searches and seizures. These intrusions into private communications are at least as invasive as the real-time wiretapping that *Berger v. New York* found was akin to a general warrant search—which the Fourth Amendment was designed to prohibit.

To prevent unjustified and invasive general warrant seizures of private communications stored in the cloud, this Comment proposes an approach akin to *Berger* that accounts for the invasiveness of collecting large amounts of revealing information that can reach back years. A warrant based on probable cause should be a baseline requirement. Additionally, enhanced particularization of the warrant's parameters should be required to ensure that the government cannot seize large amounts of nonresponsive information. Further, by establishing a protective constitutional backstop, this approach could provide an incentive for Congress to enact a modernized statutory framework that fully protects users' privacy in the cloud.

218. *See supra* notes 180–184 and accompanying text.