FOURTH AMENDMENT PARTICULARITY IN THE CLOUD

Bihter Ozedirne†

I. INTRODUCTION

As cloud storage has become cheaper and easily available, more and more people are choosing to utilize services that provide remote storage of their data. While the rapid adoption of cloud storage services has created conveniences for users, it also raises new privacy concerns, particularly with respect to government access to stored data under the Fourth Amendment.

The cloud raises some novel concerns about search and seizure. The amount of data that is available is vast and the service provider is used to execute searches. These issues are highlighted in the way courts have dealt with the particularity requirement of the Fourth Amendment, which requires a warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized."[1] This Note focuses on the Fourth Amendment and the particularity requirement. Part II explains the amendment and the general landscape of the particularity requirement, Part III provides background on how courts dealt with particularity for tangible property and electronic devices, and Part IV focuses on the various approaches courts have taken to the cloud and particularity. Part V sets forth recommendations for tackling the particularity issue and suggests how courts can minimize the amount of data that is disclosed to the government without unduly interfering with the government's investigative discretion and effectiveness, and without exposing service providers to their customers' private data.

II. FOURTH AMENDMENT AND PARTICULARITY

The Fourth Amendment ensures "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[2] It specifies that warrants may be issued only upon probable cause and supported by oath. Most importantly, for the purposes of this Note, warrants must "particularly describ[e] the place to be searched, and the persons

DOI: https://doi.org/10.15779/Z38XG9FB3K

† J.D. Candidate, 2019, University of California, Berkeley, School of Law.

1. U.S. CONST. amend. IV.
2. *Id.*

or things to be seized."[3] A recent Tenth Circuit case provides a useful metric for determining whether a warrant is sufficiently particular: "[C]onsider whether the warrant's description of items to be searched would enable the searcher to reasonably ascertain and identify the things authorized to be seized."[4]

There are a number of reasons to limit the government's search and seizure power. The Supreme Court emphasized these reasons in *Marron v. U.S.*, stating "the requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."[5] The Court has recognized that the Fourth Amendment was "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[6]

The constraints imposed by the "particularity requirement" are rather straightforward when applied to physical evidence. If, for example, officers requested a warrant for particular documents believed to be in a house, they may obtain a warrant to search the entire house, but they would not be able to request a warrant authorizing them to seize the entire contents of the home. Such a search would be too broad and would effectively enable a general search warrant. Instead, due to the particularity requirement, they would need to describe both the property to be searched as well as the kinds of documents and other property to be seized.[7]

The particularity requirement is more flexible for electronically stored information. The 2009 amendment to Rule 41 of the Federal Rules of Criminal Procedure endorses a two-step process for the search and seizure of such information. Per the rule, a warrant may authorize the seizure of electronic storage media for later review.[8] In practice this leads law enforcement agents to seize entire bodies of electronic media and review the information at a later date to determine whether it is consistent with the scope of the warrant.[9] This approach means law enforcement seizes and searches a large quantity of irrelevant but possibly very private data. This situation is likely to become more

3. *Id.*
4. United States v. Dunn, No. 15-1475, 2017 WL 6349439, at *1 (10th Cir. 2017).
5. Marron v. U.S., 275 U.S. 192, 196 (1927).
6. Riley v. California, 134 S. Ct. 2473, 2494 (2014).
7. FED. R. CRIM. P. 41(e)(2).
8. *Id.* at 41(e)(2)(B).
9. Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 7 (2015).

prevalent as individuals rely on cloud storage to serve as virtual file-cabinets and as the seize first, search later approach is extended to data in cloud storage.

This application of the rule to electronically stored data has not gone unquestioned. Magistrate Judge Facciola, from the United States District Court for the District of Columbia, expressed concern with the initial broad collection of data.[10] The 2009 amendment to Rule 41 was introduced to allow law enforcement to sort through large amounts of data, a lengthy process that justifies the two-step process of data collection.[11] Judge Facciola argues there are more efficient ways to conduct this process and the standard language in warrants "insisting that the agents must open every file and folder may simply be incorrect and therefore an illegitimate premise for the kind of searching law enforcement will actually do."[12]

III. PARTICULARITY BEFORE THE CLOUD

A. PARTICULARITY FOR PHYSICAL ITEMS

"Physical data" is used as a catchall term in this Note to encompass traditionally physical sources of data, such as documents and other tangible and non-electronic sources of evidence. A review of how courts have handled particularity in this realm is relevant to understand the evolution of particularity and determine whether aspects of these cases can be applied in the cloud context.

Various cases have provided a framework by which search warrants can comply with the particularity requirement.[13] Generally, this means both the description of the location and item(s) to be seized must be specific to some degree. For example, in *United States v. Alberts* the warrant stated that "certain large green garbage bags" were believed to be located at the residence of Linda Alberts Thompson.[14] The green bags were ultimately found and seized at the residence of Laverne Goodbird.[15] The court found nothing in the warrant that would support searching this second residence. Thus, the description "certain large green garbage bags" was not sufficient to satisfy the

10. *In re* Search of Info. Assoc. with the Facebook Account Identified by the Username Aaron.Alexis, 21 F. Supp. 3d 1, 8 (D.D.C. 2013).

11. *See* FED. R. CRIM. P. 41(e)(2).

12. *See Aaron.Alexis*, 21 F. Supp. 3d at 11.

13. *See, e.g.*, United States v. Alberts, 721 F.2d 636, 639 (8th Cir. 1983) ("A search warrant must contain a description of the place to be searched. The place must be described with sufficient particularity as to enable the executing officer to locate and identify it with reasonable effort.").

14. *Id.* at 638.

15. *Id.* at 639.

particularity requirement—the description of the garbage bags was not insufficient, but the description did not include a description of the place to be searched.[16] While the garbage bags were identified, the warrant failed to include information about where the garbage bags were located. "Such specificity is required in order to avoid any reasonable probability that another place might mistakenly be searched."[17]

In *Steele v. United States*, the Supreme Court addressed both aspects of the particularity requirement, the place to be searched and the things to be seized.[18] The warrant for the seizure of alcohol was issued after an officer had seen cases of whiskey being unloaded in front of a building.[19] The defendant claimed the building that was searched was improperly identified in the warrant as a garage and place of business. The Court disagreed, finding the description of the location accurate. The Court clarified that "it is enough if the description is such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended."[20] Additionally, the Court found the description of the property to be seized as sufficient. The warrant referred to "cases of whiskey" and although the cases that were ultimately seized may not have been the exact cases that officers saw being delivered, the Court found the description to be specific enough.[21]

A number of cases have also tackled the issue of imprecise descriptions of property to be searched. In *United States v. Brakeman,* a warrant was issued to search a mobile home.[22] The affidavit provided the address, 205 Monksdale, and a description of the property, thus identifying the place to be searched.[23] Later evidence showed this description was ambiguous; 205 Monksdale was the address of the owner of the mobile park and the defendant's neighbor and landlord. Despite the confusion, the officer was familiar with the property and only searched the defendant's mobile home. The *Brakeman* court held that the warrant's description was sufficiently particular, because it described the mobile home in detail and the defendant admitted his property was "physically" at the address listed on the affidavit.[24] The court did not take issue with the fact that the officer relied on his knowledge when executing the

16. *Id.*
17. *Id.*
18. Steele v. United States, 267 U.S. 498, 499 (1925).
19. *Id.*
20. *Id.* at 502.
21. *Id.*
22. United States v. Brakeman, 475 F.3d 1206, 1208–09 (10th Cir. 2007).
23. *Id.* at 1209.
24. *Id.* at 1211.

warrant because the officer's knowledge was not the "sole means of determining what property [was] to be searched."[25]

A number of courts have also addressed the question of particularity when the warrant provides for a rather expansive search. In *United States v. Ulbricht*, the Second Circuit made it clear that breadth and particularity are distinct concepts and that the breadth of a warrant may be wide without violating the particularity requirement. [26] The Second Circuit noted that a warrant authorizing the search of an entire home could be sufficiently particular if "there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence."[27] Similarly, in *U.S v. Bradley*, the Eleventh Circuit held that a warrant to search all of a business's records was sufficiently particular because traces of the alleged illegal activity "were likely to be found spread out amongst the myriad of records in [the company's] possession."[28]

However, the Supreme Court has noted that officials "must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."[29] Minimization is an established requirement for electronic surveillance,[30] but is less commonly discussed in the context of warrants for physical items. Even so, the Court has made it clear that court-approved restraint during a search is necessary[31] and has taken issue with other examples of surveillance where the amount of collected information was not minimized.[32]

---

25. *Id.* at 1211–12.

26. United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017).

27. *Id.*

28. United States v. Bradley, 644 F.3d 1213, 1259–60 (11th Cir. 2011).

29. Andersen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

30. 18 U.S.C. § 2518(5) (2012) ("Every order and extension . . . shall be conducted in such as a way as to minimize the interception of communications not otherwise subject to interception under this chapter.").

31.

> It is apparent that the agents in this case acted with restraint. Yet the inescapable facts is that this restraint was imposed by the agents themselves, not by a judicial officer . . . In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.

See Katz v. United States, 389 U.S. 347, 356–57 (1967).

32. *See* Berger v. New York, 388 U.S. 41, 58–60 (1967) (noting that the two-month duration of the eavesdropping and the lack of termination date was problematic, and that "the statute's blanket grant of permission to eavesdrop is without adequate judicial supervision or protective procedures").

B. PARTICULARITY FOR ELECTRONIC DEVICES

Electronic devices, such as computers, tablets, and cellphones are distinct from "physical data" because they have the ability to store vast amounts of information.[33] Due to this quality and the hectic environment in which warrants are usually served, the Federal Rules of Criminal Procedure authorize a two-step process for the search and seizure of electronically stored information.[34] Step one involves "the seizure of electronic storage media or the seizure or copying of electronically stored information," while step two involves "later review of the media or information consistent with the warrant."[35] This process is meant to address some of the practical constrains of warrant execution, such as law enforcement's inability to review the large quantity of information stored on electronic devices on site.[36]

Courts and commentators alike have recognized that seizing electronic data results in over-collection and both have struggled to balance the conflicting demands of particularity and conducting a thorough search. One proposed solution is the elimination of the plain view doctrine, which allows officers, under certain circumstances, to seize evidence in plain view without a warrant.[37] Professor Orin Kerr, who proposed this in a 2005 article[38] has, however, since rescinded the idea.[39] Kerr identified eliminating the doctrine as the simplest, yet most draconian approach, where all evidence beyond the scope of a warrant would be suppressed, thus eliminating the potential for over-collection.[40] Since then, a variety of other solutions have been put forth, which, rather than reflecting a wholesale rejection of the plain view doctrine, try to resolve the privacy concerns that originate from the doctrine in other ways. The rise of cloud storage and its growing centrality in the way businesses and individuals generate and store data and communications both exacerbates

33. *See* Kevin Golembiewski, *All Data Are Not Created Equal: Upholding the Fourth Amendment's Guarantees When Third Party Consent Meets the Shared Electronic Device*, 56 WASHBURN L.J. 35 (2017) (noting that "our smartphones, laptops, tablets, and desktop computers have the capacity to store 'millions of pages of text, thousands of pictures, or hundreds of videos.' Given this capacity and the extent to which we rely on these types of electronic devices in our daily lives, such devices 'carry a cache of sensitive personal information' that is historically unparalleled").

34. FED. R. CRIM. P. 41(e)(2)(B).

35. *Id.*

36. *Id.* at 41 (2009 Amendments).

37. *See* Coolidge v. New Hampshire, 403 U.S. 443, 444 (1971).

38. *See* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 582–83 (2005).

39. *See* Kerr, *supra* note 9 at 3–4.

40. Kerr, *supra* note 38 at 582–83.

the privacy concern and presents some unique characteristics that have not been explored fully by legal scholars.

The Supreme Court acknowledged that electronic devices are different from "physical items" in *Riley v. California.*[41] While the case centered on whether law enforcement are required to obtain a warrant to search digital information on a cell phone, the Court also discussed what makes electronic devices distinct.[42] The Court noted the capacity of devices such as cell phones to store vast amounts of data that can date back a number of years and convey more information than physical records.[43] Although the Court stated unequivocally that this information is not immune from search, it noted the different nature of cell phones.

Courts have tackled the particularity requirement in relation to electronic devices and scholarship has noted the importance of the requirement in relation to cell phone searches.[44] In *United States v. Ganias*, the Second Circuit addressed concerns about the retention of seized data.[45] Federal law enforcement were investigating Ganias's clients and seized files containing Ganias's personal financial records in the process. Officials assured Ganias his records would be purged once they searched the relevant files, but his records were retained, and law enforcement began looking into the financial irregularities found in them. After the record had been in the government's possession for two-and-a-half years, the government obtained another warrant to search and preserve Ganias's records.[46] The Second Circuit highlighted the issue of particularity, stating that "if the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed cause, every warrant to search for particular electronic data would become, in essence, a general warrant."[47] The Second Circuit later decided, en banc, that the government relied on good faith[48] and thus did not decide on whether the government violated the Fourth

41. *See* Riley v. California, 134 S. Ct. 2473, 2478 (2014).

42. *Id.* at 2477.

43. *Id.*

44. *See generally* Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585 (2016).

45. United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *aff'd*, 792 F.3d 290 (2d Cir. 2015).

46. *Id.* at 128.

47. *Id.* at 139.

48. Good faith is an exception established by the Supreme Court, whereby "the Fourth Amendment exclusionary rule should be modified so as not to bar the use in the prosecution's case in chief of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately unsupported by probable cause." *See* United States v. Leon, 468 U.S. 897, 900 (1984).

Amendment.[49] Regardless, the discussion on the applicability of the particularity requirement to seized data shows the court grappling with technological developments.

The D.C. Circuit, in *United States v. Griffith*, also addressed the unique concerns raised by the application of the particularity requirement to electronic device searches.[50] The warrant in question "authorized officers to search for and seize *all* cell phones and other electronic devices" in the defendant's residence.[51] The court was concerned that the seizure of all devices violated the particularity requirement, noting that "a warrant with an 'indiscriminate' sweep is 'constitutionally intolerable.' "[52] It ultimately held that officers lacked probable cause to seize all devices and found the warrant overbroad.[53] Although these kinds of searches are often permissible under step one of the two-step procedure in Rule 41, the court here noted a lack of probable cause. While most individuals own cellphones, the affidavit in this case did not provide any indication that the defendant owned a cell phone, or that incriminating evidence would be found on a phone.[54] The court also noted that electronic devices are distinct from other objects police may seize. Unlike items such as drugs or weapons that are obvious contraband, electronic devices are lawful objects. The "courts have allowed more latitude in connection with searches for contraband items . . . [and] the understanding is different when police seize innocuous objects."[55] The court still provided some flexibility however, stating that there are circumstances when law enforcement may have more latitude to conduct a cursory search of electronic devices to determine their relevance to the investigation, such as when they lack specific information about the make and model.[56]

In *In re Cellular Telephones*, Magistrate Judge Waxse proposed using search protocols as a way to satisfy the particularity requirement.[57] Waxse denied a search warrant to the Drug Enforcement Agency for "names, addresses, telephone numbers, text messages, digital images, video depictions, or other identification data" located on five cell phones.[58] While the court was clear that

49. United States v. Ganias, 824 F.3d 199 (2d Cir. 2016) (case decided en banc at the court's own request).

50. United States v. Griffith, 867 F.3d 1265 (D.C. Cir. 2017).

51. *Id.* at 1268 (emphasis added).

52. *Id.* at 1275.

53. *Id.* at 1277.

54. *Id.* at 1272–73.

55. *Id.* at 1276 (internal citation and quotation removed).

56. *Id.*

57. *In re* Cellular Telephones, No. L4-MJ-8017-DJW, 2014 WL 7793690, at *1 (D. Kan. 2014).

58. *Id.*

search protocols might not be necessary for all warrants, it held that in many cases "the only feasible way to specify a particular 'region' of the computer will be by specifying how to search."[59] The court felt this approach was necessary due to the amount of information that could be collected.[60]

IV. PARTICULARITY IN THE CLOUD

The cloud—or cloud computing, to be more accurate—"is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)."[61] The cloud has had revolutionary significance and "few trends in information technology (IT) have had a greater impact than the rising of cloud computing."[62] Corporations and individuals alike rely heavily on the cloud.[63] A number of companies, such as Google, Amazon, and Microsoft, also host cloud services for companies and individuals.[64] For example, Snapchat uses Google's cloud services and many consumers' e-mails, social media, and gaming services are stored on the cloud.[65] In practical terms, this means that individuals and corporations store large amounts of data with third-party service providers.[66]

The amount of information available for disclosure through cloud storage challenges courts to address privacy concerns and prevent general warrants. Courts have struggled to translate the language of the Fourth Amendment and

59. *Id.* at *8.

60. *Id.* at *11.

61. Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. STANDARDS & TECH. (NIST Special Publication 800-145, Sept. 2011), at 2.

62. Dan Cordingley, *The Next Phase of the Cloud Computing Revolution Is Here*, FORBES (Aug. 11, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/08/11/the-next-phase-of-the-cloud-computing-revolution-is-here/#6db74db46a16 [https://perma.cc/6XXU-P2QW].

63. *See* Philip Guido, *Three Companies That Transformed Their Business Using Cloud Computing*, FORBES (Nov. 3, 2014), https://www.forbes.com/sites/ibm/2014/11/03/three-companies-that-transformed-their-businesses-using-cloud-computing/#106c5b361b66 [https://perma.cc/86UV-C8G6].

64. *See, e.g.*, Barb Darrow, *How These Fortune 500 Companies Are Moving to the Cloud*, FORTUNE (July 19, 2006), http://fortune.com/2016/07/19/big-companies-many-clouds/ [https://perma.cc/UKG2-62V3]

65. *See* Quentin Hardy, *The Era of Cloud Computing*, N.Y. TIMES (June 11, 2014), https://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/ [https://perma.cc/3YDX-JKA5].

66. For example, many individuals use services like Google Drive, which provides 15 GB of free storage. *See* GOOGLE DRIVE, https://www.google.com/drive/ (last visited Mar. 18, 2018) [https://perma.cc/56HT-HHFL].

the requirements set by Rule 41 of the Federal Rules of Criminal Procedure to cloud content. This issue has not yet attracted the attention of legal scholars.

Magistrate Judge Facciola summarized the issue in a 2014 case about an Apple e-mail account search, taking issue with the breadth of the initial disclosure, which he labeled an "exploratory rummaging."[67] The Fourth Amendment's purpose is to prevent general warrants and the type of rummaging and privacy invasion that such a warrant would provide. Here, Judge Facciola feared that allowing the government to seize a large amount of e-mails for which they had not established probable cause would amount to issuing a general warrant.[68]

In addition to the matter of sheer volume, government access to cloud storage has another unique aspect: the role of the service provider. Unlike search warrants for traditionally physical data or electronic devices, warrants for cloud content are served on the service providers, who are then responsible for handling the legal process.[69] The introduction of the third-party service provider results in a very different approach to the execution of the warrant. As discussed in Part III, warrants for digital evidence stored on local devices are normally executed in two stages.[70] Warrants for cloud content present a challenge to this framework because the execution of the warrant involves a four, rather than two-step process. In the cloud context, the steps are as follows: (1) the service provider searches for the requested content; (2) the service provider seizes the content and turns it over to law enforcement; (3) law enforcement searches the content for relevant information; and (4) law enforcement seizes the relevant content. Reframing the execution steps in this manner provides a clearer framework for investigating particularity concerns.[71]

---

67. *See* Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 149 (D.D.C. 2014) *vacated sub nom.* Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157 (D.D.C. 2014).

68. *Id.* at 153.

69. *Transparency Report Help Center, Legal Process for User Data Requests FAQ*, GOOGLE, https://support.google.com/transparencyreport/answer/7381738?hl=en [https://perma.cc/J3BM-MYJF] [hereinafter *Google Transparency Report Help Center*].

70. FED. R. CRIM. P. 41(e)(2)(B) ("A warrant under Rule 41(e)(2)(B) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.").

71. *See [Redacted]@mac*, 13 F. Supp. 3d at 153 (clarifying that the two-step procedure should be a narrow exception and applied "only because there is no alternative that would allow the government to access the data for which it does have probable cause").

Courts have adopted at least four different approaches and solutions to the particularity problem: (1) the "hands off" approach; (2) the "service provider participation" approach; (3) the "ex ante restrictions" approach; and (4) the "plain view and use restrictions" approach. Some courts have chosen to apply one of these approaches, while other courts have combined multiple approaches.

A. THE "HANDS OFF" APPROACH

The "hands off" approach is exemplified by deference to the government and wariness to minimize search warrants. Minimization is a term used frequently when discussing particularity and refers to ways to limit "unwarranted intrusions upon privacy."[72] Courts that follow the "hands off" approach are likely to grant search warrants that require the disclosure of entire e-mail accounts and consider the warrant sufficiently particular regarding the "things to be seized."[73]

This approach was taken in *United States v. Bowen*, where the government executed search warrants on the defendants' e-mail accounts.[74] The court denied the defendants' motion to "suppress the results of the searches of their e-mail accounts on the grounds that the warrants authorizing those searches lacked sufficient particularity in describing the items to be seized."[75] The court held that it was "ill-suited to constrain law enforcement to certain search-terms or methodologies in advance."[76] The court reasoned that search terms would constrain the data collection in a manner that could result in law enforcement missing key information, particularly when suspects use code words or untraditional labels to code their documents.[77] The court rejected ex ante limitations on how the government handles seized data for similar reasons.[78] The court also rejected requiring the service provider to minimize data collection at the initial search and seizure stages, finding that the Fourth Amendment does not require law enforcement 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."[79]

---

72. *See* Kerr, *supra* note 9, at 18 (recommending use restrictions as a way to minimize intrusion upon privacy for computer searches).

73. *See* U.S. CONST. amend. IV.

74. United States v. Bowen, 689 F. Supp. 2d 675 (S.D.N.Y. 2010).

75. *Id.* at 68.

76. *Id.*

77. *Id.*

78. *Id.* ("To limit the government's computer search methodology ex ante would 'give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents' or other creative data concealment techniques.").

79. *Id.* at 682.

Magistrate Judge Gorenstein took a similar approach a few years later in *In the Matter of a Warrant for All Content*, this time regarding a search warrant on an e-mail account of a suspected money launderer.[80] The search warrant directed the service provider to provide "all content and other information within the Provider's possession, custody, or control associated with the e-mail account, including all e-mails sent, received, or stored in draft form, all address book information, and a variety of other information associated with the account."[81] The warrant stated that law enforcement was going to investigate the disclosed data in order to locate specific categories of evidence, but the warrant did not include a search protocol, time limit for the search, or information about the destruction of nonresponsive data.[82] Judge Gorenstein was explicit in that he did not view seizing an entire e-mail account as a general search and noted that "ample case authority sanctions some perusal . . . of documents . . . in order for the police to perceive the relevance of the documents to crime."[83] Thus, the "perusing" that would result from an initial collection would not be a general search if it was limited in some fashion. Judge Gorenstein was also clear that he would not impose a time restriction on the government because the government may need to retain the materials as the investigation unfolds.[84] Instead of establishing a new rule to address the broad collection of data, he chose to rely on existing remedies such as suppression of evidence,[85] civil damages actions, and a motion to return property under Rule 41(g).[86]

Both courts dismissed the need for a more particularized warrant by citing technical limitations and practicality concerns. The *Bowen* court dismissed the possibility of a service provider limiting the data disclosure, stating that "because of time restraints and insurmountable technical limitations, such

80. In the Matter of a Warrant for All Content & Other Info. Associated with the E-mail Account xxxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc. 33 F. Supp. 3d 386 (S.D.N.Y. 2014).

81. *Id.* at 388 (internal quotation marks omitted).

82. *Id.*

83. *Id.* at 391.

84. *Id.* at 398.

85. Evidence may be suppressed through a motion to suppress. *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 11.2 (5th ed. 2017) ("The motion to suppress is the device by which the issue of whether evidence should be excluded because obtained in violation of the Fourth Amendment is ordinarily raised in a criminal case.").

86. *Id.* at 399; FED. R. CRIM. P. 41(g) ("A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.").

searches cannot be carried out at the time the warrant is executed at the premises."[87] Judge Gorenstein took this view a step further in *In the Matter of a Warrant for All Content*, stating, "We perceive no constitutionally significant difference between the searches of hard drives . . . and searches of e-mail accounts."[88]

These courts disregarded the fundamental difference between executing search warrants for electronic devices and cloud storage. These courts' justifications address the practical concerns of executing a search warrant for devices: such a warrant is generally executed with multiple people around and in an environment that is likely to be hectic and not conducive to the careful investigation of the evidence.[89] This situation provides sufficient justification for why the seizure of an entire device, regardless of whether the device contains information beyond the scope of the warrant, still satisfies the particularity requirement. It is unlikely that law enforcement can sift through all of the information stored on a device or devices at the scene. Thus, a later review of the seized data is a practical solution.

These constraints, however, do not exist in the cloud context and the courts have committed an error in failing to acknowledge this difference. Search warrants for cloud content are not served on a suspect's premises or in a crowded environment and are not executed by law enforcement, in the traditional sense. Instead, the warrant is typically delivered to a service provider, which collects and discloses the requested data to law enforcement.[90] Thus, the concerns cited to justify the initial broad collection in the electronic devices context do not apply. Service providers are not processing these warrants in a hectic manner or in distracting conditions. The Eleventh Circuit

87. *See* United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010) (citing United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2007)).

88. *See xxxxxxx@gmail.com*, 33 F. Supp. 3d at 394.

89. *See Bowen*, 689 F.Supp.2d at 681 (noting "[I]n most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities"); xxxxxxx@gmail.com, 33 F. Supp. 3d. at 392 (noting that "[i]n the case of electronic evidence, which typically consists of enormous amounts of undifferentiated information and documents, courts have recognized that a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search").

90. *See Google Transparency Report Help Center*, *supra* note 69 ("Does Google give governments direct access to user data? We require that requests for user data be sent to Google directly . . . . What does Google do when it receives a legal request for user data? . . . When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and Google's policies. Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law.").

noted this distinction, stating, "[h]ard drive searches require time-consuming electronic forensic investigation . . . and conducting that kind of search in the defendant's home would be impractical . . . by contrast, when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data."[91] Service providers have the flexibility and time that is usually not available when executing a warrant. This markedly different environment raises questions about the justification provided in both *Bowen* and Judge Gorenstein's opinion and shows that cloud content is in fact different from electronic devices.

B. THE "SERVICE PROVIDER PARTICIPATION" APPROACH

The second approach relies on service providers to limit the amount of data provided to the government. Courts have employed two methods: (1) requiring a temporal limitation in the warrant, and (2) requiring the service provider to filter content by turning over, for example, only e-mail to or from particular persons. Some courts have chosen to implement both methods, while others only required one.[92]

The Eleventh Circuit and the Middle District of Alabama have employed temporal limitations in order to address particularity concerns. In *Blake*, the Eleventh Circuit addressed search warrants that were served on the defendant's Facebook account.[93] The warrants were part of an investigation into the members of a suspected prostitution ring.[94] The warrants required Facebook "to disclose to the government virtually every type of data," including every sent and received private instant message, every IP address that the accounts had logged in from, every uploaded photograph or photograph in which the defendant was tagged, the name of every public and private group the defendants were a member of, every search conducted on the website, every purchase made through the "Facebook Marketplace," and the defendants' entire "friends" list.[95] The warrants did not provide a timeframe by which to limit the disclosures and thus were not limited to the time period in which the alleged illegal activity occurred.[96]

The Court concluded that such broad disclosure was unnecessary and suggested alternatives that the government could have explored.[97] Instead of

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

92. *See, e.g.*, *Blake*, 868 F.3d 960.

93. *Id.* at 967.

94. *Id.* at 966.

95. *Id.*

96. *Id.* ("[O]ne warrant asked for all data 'from the period of the creation of the account' and the other did not specify what period of time was requested.").

97. *Id.* at 974.

requesting all private messages, the Court suggested the warrants could have "limited the request to messages sent to or from persons suspected at that time . . . [and] should have requested data only from the period of time during which [the defendant] was suspected of taking part in the prostitution conspiracy."[98]

The Court also rejected an oft-used justification for this type of broad collection, that searches of this kind are time-consuming and the initial over-collection is necessary to conduct the search in a calmer environment.[99] The Court acknowledged that these concerns are not entirely present in the cloud context.[100] Nevertheless, the court ultimately affirmed the district court's decision not to suppress the evidence.[101] The court acknowledged "the warrants may have violated the particularity requirement," but did not find it unequivocally so because "the warrants were not so facially deficient that the FBI agents who executed them could not have reasonably believed them to be valid."[102]

The Middle District of Alabama also required a temporal limitation on a search warrant seeking cloud content, this time in a case involving a scheme to defraud using stolen identities.[103] The search warrant in question sought "the contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account," session and IP information, address book information, and all location data, among other types of content.[104] Citing *Blake*, the court took issue with the lack of temporal limitations and required that the warrants prohibit the disclosure of account data prior to January 1, 2015.[105] In addition to a broad temporal limitation, the court also required a stricter limitation to be implemented on a case-by-case basis. This stricter limitation was "based on an assumption that data from three months before the first activity the Government currently has evidence of, and the three months after the last, would more particularly describe the time

98. *Id.*

99. *Id.*

100. *Id.* at 974 ("Hard drive searches require time-consuming electronic forensic investigation with special equipment, and conducting that kind of search in the defendant's home would be impractical . . . when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data.").

101. *Id.*

102. *Id.* (internal quotes omitted).

103. United States v. Search of Info. Assoc. with Fifteen E-mail Addresses, No. 2:17-CM-3152-WC, 2017 WL 4322826, at *1 (M.D. Ala. Sept. 28, 2017).

104. *Id.* at *2–3.

105. *Id.* at *5.

period of information to be searched."[106] The court did not provide further guidance on how to implement this case-by-case search.

Both courts provided similar reasons for imposing a temporal restriction. They noted the amount of disclosed data was troubling[107] and the Alabama court also found the government had not established probable cause for a disclosure beyond a certain date range.[108] Both courts highlighted that the main issue with the "hands off" approach was that it would allow the search of e-mail accounts from the time of their creation, and instead proposed a limitation that is straightforward and simple to apply and does not require the service provider to play a very active role. A service provider can implement a temporal limitation without expertise on investigative techniques or knowledge of the crime at hand.

In these cases, the government was willing to accept temporal limits, at least when pressed by judges. In fact, in the Alabama case, the government itself proposed limiting the timeframe of the initial collection.[109] This is a significant development and bodes well for the potential standardization of temporal limitations.

The Eleventh Circuit in *Blake* and a number of district courts have proposed additional methods of satisfying the particularity requirement through the service provider.[110] These methods require the provider to take a more involved approach and restrict the content that is being disclosed at a finer level.[111] While temporal restrictions only require the service provider to select a timeframe, these additional methods require the provider to determine which content is responsive to the search warrant. This could take the form of

106. *Id.* at *6.

107. *See* United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017); *see also Fifteen E-mail Addresses*, 2017 WL 4322826, at *6.

108. *Fifteen E-mail Addresses*, 2017 WL 4322826, at *7.

109. *Id.* at *14.

110. *See* United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010); United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013); United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010); United States v. Khanani, 502 F.3d 1281, 1290–91 (11th Cir. 2007).

111.

> With respect to private instant messages, for example, the warrants could have limited the request to messages sent to or from persons suspected at that time of being prostitutes or customers. And the warrants should have requested data only from the period of time during which Moore was suspected of taking part in the prostitution conspiracy. Disclosures consistent with those limitations might then have provided probable cause for a broader, although still targeted, search of Moore's Facebook account.

See Blake, 868 F.3d at 974.

filtering e-mails to and from certain individuals, or other methods. Regardless of the specific method, they all place the initial responsibility of determining the responsiveness of the content on the service provider.

Other courts have been a bit clearer and more proactive in the type of content that service providers should screen. The *Blake* court stated the warrants should have been limited to messages sent to or from suspected persons,[112] while the District of the District of Columbia in *Aaron.Alexis* ordered Facebook to limit disclosure to "information about [the suspect's] account and the content of messages that he sent" and to only disclose records of communication between third parties, rather than the content of the communications.[113]

The same court proposed an even more proactive approach a year later, in an order that was ultimately vacated.[114] Nevertheless, the order presented a new and unique approach that is worth exploring. The case involved a search warrant where the government requested all information associated with an Apple e-mail account within a certain timeframe.[115] Despite the temporal limitation, the judge took issue with the breadth of the initial disclosure, labeling the government's request a "general warrant," or an "exploratory rummaging in a person's belongings."[116] Because the court defined any e-mail turned over to the government as "seized," it required the government to establish probable cause, not only for the account in question, but the individual disclosed messages.[117] The court's proposed solution involved the service provider, Apple, conducting the initial search of the account and turning over only the relevant data it discovered.[118] The court felt the Fourth Amendment required this approach "because nothing else will eliminate the present certainty that the government will unconstitutionally seize data for which it has not established probable cause to seize."[119]

These restrictions present interesting options to meet the particularity requirement. It is important to note, however, that placing these restrictions

112. *See id.*

113. *In re* Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 5 (D.D.C. 2013).

114. Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145 (D.D.C. 2014), *vacated sub nom.* Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157 (D.D.C. 2014).

115. *[Redacted]@mac*, 13 F. Supp. 3d at 145, 139.

116. *Id.* at 149.

117. *Id.*

118. *Id.* at 153.

119. *Id.* at 154.

on the service provider presents a number of issues. First, the employees that handle data disclosure requests at service providers are usually legal assistants who are not trained in law enforcement investigative techniques.[120] Therefore, either the warrant requiring their active involvement in content minimization would have to include detailed instructions on how to comply, or they would have to be trained to properly execute the warrant. Second, service providers would be required to build out a very specialized infrastructure enabling them to adequately execute these warrants. Many service providers have a data disclosure system in place,[121] but it likely prohibits employees from actively engaging with user content when responding to warrants. A restriction on employee exposure to user content is important. While service provider access is beyond the purview of the Fourth Amendment, it is an important privacy consideration that should not be disregarded while considering other privacy concerns. Regardless, service provider filtering is a valid limitation to explore as it does tackle concerns over the initial broad collection of cloud warrants.

C. THE "EX ANTE RESTRICTIONS" APPROACH

The third approach utilized by courts is ex ante restrictions. This approach places restrictions on how the government handles data once it is turned over by search providers. Restrictions are placed during step two of Rule 41. Courts that follow this approach either require the inclusion of search protocols in the warrant or a declaration that all records that are beyond the scope of the investigation will be returned to the service provider or destroyed.

The use of written search protocols is not a novel concept in the courts. A number of circuit courts have addressed the issue, though not in the cloud context. The Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, upheld the inclusion of search protocols, while the Second, Seventh, and Eleventh Circuits have struck down their required inclusion.[122]

District courts have addressed this issue within the cloud context. Judge Facciola [123] advocated for search protocols to satisfy the particularity

120. The author served as a Legal Assistant at one of these service providers and is thus familiar with the training provided at, at least, one company that receives search warrants for content.

121. *See, e.g.*, *Google Transparency Report Help Center, supra* note 69; *Government Requests Report*, FACEBOOK, (https://govtrequests.facebook.com/country/United%20States/2016-H2/) [https://perma.cc/4LNG-FEXY].

122. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010); United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013); United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010); United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007).

123. Judge Facciola recently retired from the bench. *See* Mary Mack, *Ediscovery Expert, Retired Judge John M. Facciola, Joins Sunblock Systems' Special Masters Group*, ASS'N CERTIFIED E-

requirement, stating he would only approve the two-step procedure for conducting a search and seizure "if the government provides an adequate protocol explaining how it will perform the search."[124] Other judges have explored different options in order to satisfy the requirement.[125] For example, in *Target E-mail Accounts*, the warrants at hand requested disclosure from multiple service providers, including all e-mails, instant messages, and chat logs, for defendants suspected of knowingly purchasing stolen goods.[126] The court suggested "appointing a special master with authority to hire an independent vendor to use computerized search techniques . . . or setting up a filter group or taint-team[127] to review the information for relevance and privilege."[128] Although the court left the decision of an appropriate procedural safeguard to the government, it did make clear that some safeguard was necessary.[129] It is unclear why the court chose to leave discretion on this matter to the government. It is possible the court was proceeding cautiously due to minimal case law[130] and was struggling to maintain the balance between law enforcement's ability to investigate and Fourth Amendment rights.[131]

DISCOVERY SPECIALISTS (Jan. 25, 2017), https://www.aceds.org/news/327724/eDiscovery-expert-Retired-Judge-John-M.-Facciola-Joins-SunBlock-Systems-Special-Masters-Group.htm [https://perma.cc/3ZSH-FTZ9].

124. *See* Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 153 (D.D.C. 2014).

125. *See In re* Applications for Search Warrants for Info. Assoc. with Target E-mail Accounts/Skype Accounts (*Target E-mail Accounts*), No. 13-MJ-81630-JPO, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).

126. *Id.* at *1.

127. *Government "Taint Teams" May Open a Pandora's Box: Protecting Your Electronic Records in the Event of an Investigation*, WILMERHALE PUBLICATION & NEWS (May 11, 2004), https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=94347 [https://perma.cc/9X45-48YE] (A taint-team is a group of reviewing prosecutors and agents. They are referred to as a taint-team "because their purpose is to shield the government from a defense motion to suppress electronic record evidence based on an argument that the prosecution and investigating team was 'tainted' by viewing electronic records it had no right to see.").

128. *See Target E-mail Accounts*, 2013 WL 4647554 at *10.

129. *Id.* ("Only with some such safeguard will the Fourth Amendment's protection against general warrants be insured.").

130. *Id.* at *7 ("The Court was able to locate only a few other cases involving a search warrant served on an electronic communications service provider for the contents of an e-mail account.").

131. *Id.* at *9 ("[T]here must be an appropriate balance between allowing law enforcement to do its job effectively and protecting the Fourth Amendment rights of those being investigated.").

Similarly, in *Fifteen E-mail Accounts*,[132] the Middle District of Alabama also emphasized search protocols, though it did not require court pre-approval for the protocols.[133] The Alabama court also highlighted the main issue driving the discussion around search protocols and minimization efforts in general; a desire to "restrict [the government] . . . to uncover only information for which the Government has probable cause."[134]

The purpose of ex ante restrictions is clear: they are meant to limit the government's exposure to user information that is beyond the scope of the warrant. Whether they are desirable is up for debate. The Middle District of Alabama noted the Supreme Court's instruction that "the manner in which a warrant is executed is subjected to later review as to its reasonableness."[135] According to this view, ex ante restrictions are not required under the Fourth Amendment. Other courts are concerned about the investigative process and interfering with law enforcement's discretion.[136] Both concerns are valid, particularly as ex ante restrictions are determined before law enforcement can look at the data. Though investigators likely have information on the things to be seized, they may not be able to predict the format of how the information is organized. This makes search protocols, particularly those involving key words, problematic. A filter group, or taint team, may be the better option though there are some practical constrains with this method as well. For example, a filter group is removed from the main investigation and thus may not be as familiar with the details of the case. This may result in a less thorough or effective search. Unfortunately, there are no examples of courts setting this as a requirement, so it is unclear whether these theoretical concerns are actually the reality.

D. THE "PLAIN VIEW AND USE RESTRICTIONS" APPROACH

The final approach involves either waiving government reliance on the plain view doctrine or placing use restrictions on the collected data. This approach is meant to limit the kinds of information that law enforcement can use against the defendant. The first component of this approach, the plain view doctrine, applies when a police officer "had a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence

132. United States v. Search of Info. Assoc. with Fifteen E-mail Addresses, No. 2:17-CM-3152-WC, 2017 WL 4322826 (M.D. Ala. Sept. 28, 2017). *See supra* Part III(B).

133. *See* United States v. Search of Info. Assoc. with Fifteen E-mail Addresses, No. 2:17-CM-3152-WC, 2017 WL 4322826, at *22 (M.D. Ala. Sept. 28, 2017).

134. *Id.*

135. *Id.* at *10 (citing Dalia v. United States, 441 U.S. 238 (1979).

136. United States v. Kanodia, No. CR 15-10131-NMG, 2016 WL 3166370, at *1 (D. Mass. June 6, 2016).

incriminating the accused. The doctrine serves to supplement the prior justification . . . and permits the warrantless seizure."[137] The doctrine is very relevant in cloud searches where a large amount of information is seized because "the technology lets the government see everything, and the plain view exception then lets the government use (almost) everything."[138] The initial collection of data, while beyond the scope of the warrant, may fall under the plain view doctrine.

The second component of this approach is a use restriction that requires the destruction of nonresponsive data. There is overlap with the ex ante approach, but the limitations espoused in each approach are distinct. While ex ante restrictions impact how law enforcement agents search the collected information by limiting what they see in the first place, the elimination of plain view and use restrictions limit what law enforcement can do with the information once they see it.

Some judges have advocated for a waiver of the plain view doctrine in searches of electronically stored data. Judge Kozinski, formerly of the Ninth Circuit, expressed this clearly in his concurrence in *United States v. CDT*, stating, "magistrate judges should insist that the government waive reliance upon plain view doctrine in digital evidence cases."[139] Judge Facciola cited this statement and noted the potential for abuse of the plain view exception.[140] Despite this potential for abuse, Facciola noted that waiving the plain view doctrine would not cure the problem of over-seizure.[141]

Some district courts have advocated for a use restriction that would require the destruction of nonresponsive data.[142] These courts request law enforcement to destroy or return data that is nonresponsive and outside the scope of the warrant.[143] Much like search protocols, this restriction is also an effort to limit the amount of content the government is exposed to and "protect the purpose of the Fourth Amendment."[144] It would prevent the kind

137. Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

138. *See* Kerr, *supra* note 9, at 19.

139. United States v. Comprehensive Drug Testing, Inc. 621 F.3d 1162 (9th Cir. 2010).

140. *See* Matter of Search of Info. Associated with [Redacted]{@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 156 n.15 (D.D.C. 2014), *vacated*, 13 F. Supp. 3d 157 (2014).

141. *Id.* "[T]he government will still have the data and, even if it does not directly use it as evidence for a criminal prosecution, it may use it for other purposes.").

142. *See* In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis (*Aaron.Alexis*), 21 F. Supp. 3d 1, 10 (D.D.C. 2013); *[Redacted@mac]*, 13 F. Supp. 3d at 156.

143. *Aaron.Alexis*, 21 F. Supp. 3d at 10; *[Redacted@mac]*, 13 F. Supp. 3d at 156.

144. *See Aaron. Alexis*, 21. F. Supp. 3d at 10 ("[M]inimization procedures may be an appropriate way to protect the purpose of the Fourth Amendment even when changes in

of activity that occurred in *United States v. Ganias*, where law enforcement agents seized documents from Ganias in order to investigate his clients.[145] The agents came across discrepancies in Ganias's personal documents, which were also seized, and obtained a warrant to search Ganias's personal records.[146] Concerns about this kind of activity were expressed in *In the Matter of the Search of Information Associated with [Redacted]@mac.com*, where the court stated that keeping nonresponsive data indefinitely is similar to keeping the entire contents of a physical search because one or two pieces of paper show evidence of a crime.[147] The court was adamant that "if the government seizes data it knows is outside the scope of the warrant, it must either destroy the data or return it. It cannot simply keep it."[148]

The elimination of the plain view doctrine alone may be problematic. Professor Kerr, who once advocated for eliminating the plain view doctrine for electronic devices, has since moved away from the position and instead recommends imposing use restrictions as a way to combat the privacy concerns raised by executing warrants for digital evidence.[149] Kerr had previously explored the idea that eliminating plain view for computer searches could address the concern that these warrants were functioning similarly to general warrants.[150] Kerr's reluctance to eliminate the plain view doctrine stems from complications raised by the search and seizure of electronic data. He considers the scope of plain view, for example, and asks whether "the doctrine ever app[lies] to a second seizure—a seizure of property already seized?"[151] If we assume that the seizure of data at step one of Rule 41 is a seizure under the Fourth Amendment, would the search and seizure of the data during step two be considered a second seizure? If so, determining whether plain view applies is highly significant because eliminating the exception could result in the exclusion of the data.

Kerr provides three possibilities of how plain view would be affected under different interpretations of seizure.[152] If using the data is not considered an additional seizure then law enforcement can use the nonresponsive data,

technology dramatically change the way in which search and seizures actually occur in the real world.").

145. United States v. Ganias, 755 F.3d 125, 128 (2d Cir. 2014).

146. *Id.*

147. *See Redacted@mac,* 13 F. Supp. 3d at 156, *vacated*, 13 F. Supp. 3d 157 (2014).

148. *Id.*

149. *See* Kerr, *supra* note 9, at 17.

150. *See* Orin Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 314 (2005).

151. *See* Kerr, *supra* note 9, at 22.

152. *Id.* at 23.

making the plain view exception irrelevant. If copying the data constitutes an additional seizure then law enforcement would have to obtain a second warrant, thus the plain view exception would have a moderate effect.[153] If, however, "the data observed outside of the warrant constitutes an additional seizure . . . eliminating the plain view exception imposes the desired restriction."[154] Although this may seem like a solution, Kerr is wary of embracing this approach because its broad view of seizure "might have substantial unintended consequences."[155] This is just one example of the complications that Kerr predicts could arise, which is why he believes "imposing use restrictions on nonresponsive files is the best way to reconcile the government's need to search for responsive evidence with the Fourth Amendment command to avoid general warrants."[156]

This "plain view and use restrictions" approach addresses concerns that go beyond particularity, such as the government's use of non-relevant data collected in overly broad seizures. Although courts discuss the plain view and use restrictions approach under the framework of particularity, the approach does not address what the requirement is actually about. The particularity requirement is meant to prevent the execution of a general warrant. Although the issues of plain view and use restrictions are important for a broader privacy discussion, they do not address the ultimate concern of particularity: overbroad searches.

V. RECOMMENDATIONS

The cases above show courts struggling with how to apply the particularity requirement to new technology and exploring avenues beyond particularity to address privacy concerns. This Note endorses temporal limitations, service provider participation through content restrictions, and a service restriction that has not been considered by the courts discussed in this Note in Part IV. It does not recommend ex ante, plain view, and use restrictions at this time, as the ultimate goal of the recommendations is to narrow the scope of the initial search in order to prevent overbroad searches.

First, temporal limitations are recommended because this kind of limit is straightforward and can be implemented without too much service provider exposure to user data. The temporal restrictions should reflect the time period

153. *Id.* at 23.

154. *Id.* at 23.

155. *Id.* at 24; *see generally* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 705–09 (discussing the definition of seizure for computer data).

156. *Id.* at 17.

in which the alleged illegal activity occurred and will thus limit the breadth of the initial collection. Other scholars have made similar recommendations.[157]

The following hypothetical illustrates when a temporal limitation is appropriate. Imagine law enforcement agents suspect Suzie Q of wire fraud and they have evidence that this activity started in March 2017. If law enforcement requested a search of Suzie's e-mail account from its inception in 2005 to the present, it would be an overbroad collection and would fail to satisfy the particularity requirement. In such an instance, law enforcement does not have probable cause for the e-mails created years before the illegal activity prior and could satisfy the particularity requirement by describing the "things to be seized" as the e-mails from a few years before the illegal activity to March 2017 to present.

The second recommend approach is service provider participation through content restrictions, such as e-mails sent to and from particular e-mail addresses.[158] As with all minimization efforts, this approach should be used where applicable. It may take time for providers to implement tools that can sort through user accounts. Such tools should be automated to eliminate the exposure of content to the service provider. Though the implementation is potentially trickier than the temporal limitation, it is likely something that service providers can provide if required to do so. This is the most service provider involvement recommended as there are valid privacy concerns with allowing service providers to actively engage with user content. This approach, like the one endorsed before, can also be achieved without exposing the service provider's employees to user content and serves to restrict the amount of data initially disclosed.

Now imagine a different hypothetical: Law enforcement may or may not know the timeframe of Suzie's alleged activity, but they know that she is working with one other party, whose e-mail account has already been identified. In such an instance, it would be appropriate for the search warrant to only allow the seizure of e-mails to and from Suzie and the other party.

Over-collection could be addressed by requiring probable cause for different cloud services. This framework would require warrants to list particular cloud services and provide probable cause for each service. A similar

157. Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-mail Surveillance*, 90 NEB. L. REV. 971, 991 (2012) ("Furthermore, the government should seize only those stored e-mails and files sent or received during the time period the evidence suggests the criminal activity occurred.").

158. Other scholars have made similar recommendations. *See id.* at 1013 ("[R]equiring ISPs to segregate sought-after e-mails that are particularly described in warrants from those e-mails the government does not have probable cause to seize ensures constitutional reasonableness. . . .").

approach has been raised in the context of cell phone searches.[159] This approach is feasible because many cloud services are linked to one main account, a feature that makes the process easier for law enforcement because they only need one identifier, and because probability and particularity can often overlap.[160] This would limit the amount of data disclosed and insure that less responsive data is not being provided to the government, thus reducing the concerns that the fourth approach tries to address. Although this limitation would not include ex ante search protocols, it addresses some of the scope concerns.

Scholars, such as Kerr, fail to take into account the privacy concerns raised by the first disclosure of data. He states that "courts should not impose a limit at the physical search stage," but his proposed solution does not address the privacy concerns that are raised by this initial collection.[161] The mere looking at data, even if there is no arrest, is a privacy invasion from an individual's perspective. A vast amount of information has still been seized, regardless of whether evidence of criminal conduct is found. If the particularity requirement was applied in a more granular fashion, this concern would be alleviated by the reduction of the initial disclosure. Thus, eliminating plain view or applying use restrictions does not solve the problem that particularity is supposed to address.

An application of Suzie's hypothetical to the service-by-service shows how it can be successfully implemented. Assume Suzie uses Google for various services. This restriction would require law enforcement to provide probable cause for each of Google's services that Suzy uses. It is possible to imagine that there is probable cause for her e-mail and Drive account considering the types of services one engaged in wire fraud may utilize. It is unlikely, however, that Suzie's scheme extends to the Google Photos service. Unless law enforcement has probable cause for this content, Suzie's private photos would be protected from seizure.

The "use restrictions" approach for nonresponsive data is also recommended. The destruction of nonresponsive evidence would eliminate

159. Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 592 (noting that "magistrates can restrict warrants to the particular cell phone application for which there is probable cause").

160. *See* Friess, *supra* note 157, at 985 (2012) ("Probable cause and particularity work hand-in-hand: to establish probable cause for the issuance of a warrant, the government must demonstrate the described items are connected with the criminal activity under investigation and the items are to be found in the place to be searched. The less precise the description of the things to be seized, the more likely it will be that one or both of those probabilities has not been established.").

161. *Id.* at 11.

the concern that cloud content searches are functioning similarly to general warrants.[162] Kerr's suggestion that nonresponsive data be destroyed in the course of a search is also an effective way to implement this requirement.[163]

Suzie's hypothetical is helpful in elaborating this approach as well. Assume Suzie's e-mail account has been seized in connection with insider trading. Officers come across e-mails from her health provider during the course of the search. These e-mails are nonresponsive data and should be destroyed once discovered.

While many of the recommendations are similar to ones proposed by various courts, this Note is wary of recommending ex ante and plain view restrictions. Both approaches have the potential to impair law enforcement investigations in a manner that the other approaches do not. While the recommended approaches admittedly reduce the amount of disclosed content, they do not restrict law enforcement's to investigate in the same manner. Some scholars have suggested addressing use restrictions by treating queries like traditional searches.[164] Queries are questions that are used to retrieve specific information from a database.[165] Although this is an interesting argument, it may be difficult to apply in practice because it does not address the concerns raised by opponents of use restrictions; treating queries like searches may be difficult in instances where a defendant is using code words or untraditional labels. Additionally, this restriction and others do not address the initial issue of over-collection.[166]

VI. CONCLUSION

The Supreme Court held in *Riley* that digital storage devices are different.[167] The same is true for information stored on the cloud, not only because of the

162. Kerr, *supra* note 9, at 17.

163. *Id.* at 18.

164. Emily Berman, *When Database Queries are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 612 (2017) ("[W]hen queries result in revelations that the Supreme Court has held would violate an expectation of privacy if achieved through collection, that query is a search. In such cases, the reasonable expectation of privacy is no less violated because it was accomplished through a query rather than a more traditional search.").

165. *Query Language*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/technology/query-language [https://perma.cc/52A7-AWP3] (last visited Mar. 1, 2019).

166. *See* Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 187 ("[C]ourts and legislatures may abandon efforts to control or regulate the surveillance itself and instead limit government use of the information . . . in the long term [this reaction] will almost certainly decrease the pressure on courts and legislatures to craft meaningful restrictions on data collection.").

167. *See* Riley v. California, 134 S. Ct. 2473 (2014).

volume of information involved, but also because of the participation of the third-party service provider. Courts should utilize the providers to satisfy the particularity requirement. As Kerr stated, "[the service provider is] no longer a significant limit" and can be an effective arm to achieving the requirement that a warrant must describe with particularity the things to be seized.[168]

No single approach will provide the perfect solution for satisfying the particularity requirement for the cloud. Sometimes a temporal limitation is sufficient and sometimes a more robust restriction is needed. Different limits should be used depending on the cloud services that are being searched and the facts of the investigation. This will likely mean that magistrates need to be a bit more knowledgeable of services, while also striking a balance between protecting privacy and effective law enforcement.

168. *See* Kerr, *supra* note 9, at 15.