LOST IN THE CLOUD: THE SCOPE OF THE PRIVATE SEARCH DOCTRINE IN A CLOUD-CONNECTED WORLD

Aya Hoffman†

CONTENTS

INTRODUCTION

In 2017, the "Internet of Things" was estimated to include over twenty billion internet-connected devices across the globe.[1] American courts have recognized a "reasonable expectation of privacy" extending to the contents of computers and digital storage devices.[2] However, the extent of Fourth Amendment protection over these devices has not been

† J.D. Candidate, Syracuse University College of Law, 2018; M.S. Forensic Science Candidate, Syracuse University, 2018; B.S. Television-Radio and B.A. Anthropology, *summa cum laude*, Ithaca College, 2012. I wish to thank my husband, Shane Bucher, whose inexhaustible patience and support makes all things possible.

1. IHS MARKIT, IOT TREND WATCH 2017, 2 (2017) (ebook), https://www.ihs.com/info/0117/IoT-Trend-Watch-2017.html. The Internet of Things (IoT) is a "conceptual framework" for discussing embedded connectivity. *Id.* at 1. An IoT device is defined as a device that "has some form of embedded connectivity that allows it to directly connect to the internet or an IP-addressable device." *Id.* In addition to computers, communication, and consumer products, the IoT also includes automotive, military, industrial and medical devices. *Id.* at 2.

2. *See, e.g.*, Riley v. California, 134 S. Ct. 2437, 2493–95 (2014).

clearly delineated, particularly within the context of cloud-connected technology. As cloud storage becomes the predominant method of data storage, the establishment of clear rules regarding an individual's Fourth Amendment rights in the cloud becomes increasingly important.

In contrast to "local" storage, which requires a physical connection to the user's computer, data saved in the "cloud" is stored in data pools across multiple servers, accessible through an internet connection.[3] Often, cloud servers are not even located in the same state or country as the devices to which they are linked.[4] Moreover, personal data may be consolidated and linked across multiple devices and platforms, increasing accessibility of data from any single entry point.[5] Users can access their data in the cloud remotely, through web-based content management systems or desktop applications.[6] Furthermore, cloud storage allows for multi-point, multi-user access, which enables third-party modification of data in shared cloud storage.[7] These changes can directly affect information displayed on other connected devices.[8]

The "private search doctrine" is an exception to the Fourth Amendment's prohibition on warrantless searches, stemming from the amendment's requirement of "governmental action."[9] This doctrine permits a warrantless secondary government search when it does not exceed the scope of the initial private search.[10] Where the initial private search of a computer or digital device was not comprehensive, applying the private search doctrine to permit an unlimited secondary governmental search of the contents of that device is unconstitutional.[11]

The goal of this Note is to examine the scope of the Fourth Amendment's private search doctrine in the cloud storage context. This Note argues that the "data-based" theory, adopted by the Sixth and Eleventh Circuits, properly limits the scope of a secondary government search, as compared to the overbroad "disk-based" theory applied by the Fifth and Seventh Circuits.

3. *See* Darren Quick & Kim-Kwang Raymond Choo, *Forensic Collection of Cloud Storage Data: Does the Act of Collection Result in Changes to the Data or its Metadata?*, 10 DIGITAL INVESTIGATION 266, 266 (2013).

4. *See id.* at 267.

5. *See id.* at 266.

6. *Id.* at 267.

7. *See* DARREN QUICK, BEN MARTINI, & KIM-KWANG RAYMOND CHOO, CLOUD STORAGE FORENSICS 5 (Brett Shavers ed. 2014)).

8. *Id.*

9. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921); United States v. Jacobsen, 466 U.S. 109, 129–30 (1984) (White, J., concurring).

10. *See Jacobsen*, 466 U.S. at 121–22 (majority opinion).

11. *See id.*

Part I provides an overview of the Constitutional protection against government searches established in the Fourth Amendment and applied by the Supreme Court. Part II explains the structure and capabilities of cloud systems, with emphasis on cloud storage technology, and related issues in digital forensics. Part III examines the Circuit split between the "disk-based" and "data-based" theories of scope, in the context of the private search doctrine. Part IV applies these competing interpretations to cloud storage scenarios and explains why the "data-based" theory is best suited to modern scenarios and most consistent with the meaning of the Constitution and Supreme Court precedents.

I. HISTORY OF THE FOURTH AMENDMENT AND THE PRIVATE SEARCH DOCTRINE

A. The Fourth Amendment

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[12]

The Supreme Court has articulated two distinct types of expectations protected by the Fourth Amendment—one related to "searches" and another involving "seizures."[13] "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."[14]

The Supreme Court addressed the issue of what government conduct constitutes a "search" within the meaning of the Fourth Amendment in *Katz v. United States*.[15] In that case, the petitioner was convicted of a betting offense based on telephone conversations, which were overheard by FBI agents using an electronic listening device attached to a public telephone booth.[16] That evidence was admitted at trial, over the

12. U.S. CONST. amend. IV.

13. *See Jacobsen*, 466 U.S. at 113 (1984) ("A 'search' occurs whenever an expectation of privacy that society is prepared to consider reasonable is infringed."); California v. Hodari D., 499 U.S. 621, 625–26, 647 (1991) (defining seizure of a person to include both application of physical force and submission by the citizen to a show of authority).

14. Riley v. California, 134 S. Ct. 2473, 2482 (2014) (citing Kentucky v. King, 563 U.S. 452, 460 (2011)); *see* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

15. 389 U.S. at 354–56.

16. Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966).

petitioner's objection, and the Court of Appeals had affirmed the trial court's decision.[17] On appeal, the Court reversed, finding that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied."[18]

In a concurring opinion, Justice Harlan articulated a two-fold description of the Fourth Amendment's protections.[19] From his perspective, the Fourth Amendment required "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable."[20] Since *Katz*, the Court has consistently emphasized that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[21]

B. "Searches" of Digital Devices

In *Searches and Seizures in a Digital World*, Professor Orin Kerr[22] discussed several important distinctions between physical and digital searches, which carry further implications for the application of the Fourth Amendment.[23] "The traditional focal point of Fourth Amendment law is physical entry into a home. Homes offer predictable, specific, and discrete physical regions for physical searches . . . . The basic mechanism is walking into a physical space, observing, and moving items to expose additional property to visual observation."[24] In contrast, digital storage devices come in many physical forms, but perform the same basic function, "stor[ing] zeros and ones that a computer can convert into letters, numbers, and symbols."[25] Whereas homes are partitioned into rooms, a computer hard drive is divided into "clusters" in which files are stored.[26] The clusters are indexed such that the computer can consult the "master list" to find the physical location of the cluster within the hard

17. *Id.* at 134–36.

18. *Katz*, 389 U.S. at 353, 359.

19. *See id.* at 361 (Harlan, J., concurring).

20. *Id.* (internal quotation marks omitted).

21. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

22. Professor Kerr is the Fred C. Stevenson Research Professor of Law at the George Washington University Law School, where he is also Director of the Cybersecurity Law Initiative. *Orin S. Kerr*, GEO. WASH. L., https://www.law.gwu.edu/orin-s-kerr (last visited Oct. 22, 2017).

23. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538–47 (2005).

24. *Id.* at 538 (citing United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972)).

25. *Id.*

26. *Id.* at 539.

drive and read the correct file.[27] Thus, in contrast to a physical search of a home, retrieving digital data involves "entering commands that copy data from the magnetic discs, process it, and send it to the user."[28] These factual differences between physical searches of a home and digital searches of a computer, based on "the environment, the copying process, the storage mechanism, and the retrieval mechanism[,]" create ambiguity as to the application of Fourth Amendment principles.[29]

"Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information."[30] Yet, it is "this very quantity and variety of information [that] increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized."[31] Although the computer-as-container framework "may make conceptual sense when discussing small electronic storage devices . . . the analogy becomes strained when applied to computers with larger storage capacities[,]" like cloud storage.[32]

The Supreme Court addressed searches of digital devices head-on in *Riley v. California*.[33] *Riley* involved two cases in which police seized the petitioners' cell phones subsequent to their arrest and examined the phones without a warrant.[34] In both cases, evidence discovered on the phones was used to support the petitioners' convictions.[35] On the consolidated appeal, the Court addressed "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[36] The Court held that the government interests of officer safety and prevention of the destruction of evidence did not justify dispensing with the warrant requirement for searches of cell phone data.[37]

While noting that the exception to the warrant requirement for searches incident to arrest "has been recognized for a century," the

27. *Id.* at 540.

28. Kerr, *supra* note 23, at 540.

29. *Id.* at 538.

30. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75, 105 (1994).

31. *Id.*

32. *Id.* at 82.

33. *See* 134 S. Ct. 2473, 2480 (2014).

34. *Id.* at 2480–81.

35. *Id.*

36. *Id.* at 2480.

37. *See id.* at 2493–95.

Court's discussion focused on the scope of that exception with respect to modern cell phones.[38] In the absence of precise Constitutional guidance, the Court applied a balancing test to determine whether the exception to the warrant requirement was applicable in such circumstances.[39] This test weighs "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests."[40]

Having previously balanced these factors in *United States v. Robinson*, the Court had recognized a "categorical rule" creating an exception to the warrant requirement for searches of physical objects seized incident to arrest.[41] However, when considering these interests in the context of cell phones, the *Riley* Court determined that the rationales underpinning its decision in *Robinson* had little force.[42] The application of the rule in *Robinson* was justified by the serious risks of harm to police officers and destruction of evidence presented by physical objects, but the Court found "[t]here are no comparable risks when the search is of digital data."[43] Thus, the *Riley* Court distinguished cell phones from other physical objects, noting that "[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals . . . [and a] search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*."[44]

The government's primary concern was preventing the destruction of evidence due to the possibility of data encryption or remote wiping.[45] Data encryption involves the use of algorithmic processes to render data virtually unreadable without the use of a key.[46] It is possible for a third party to trigger a remote wipe, or a device can be pre-programmed to automatically delete data based on a geographical trigger.[47] However, both methods require that the phone is connected to a wireless network.[48] The Court dismissed both arguments, noting that "[i]f the police are truly

38. *Riley*, 134 S. Ct. at 2482, 2484.

39. *See id.* (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

40. *Id.* at 2484 (quoting *Houghton*, 526 U.S. at 300).

41. *Id.*

42. *Id.*

43. *Riley*, 134 S. Ct. at 2484–85.

44. *Id.* at 2485.

45. *Id.* at 2486.

46. *See* Thomas J. Smedinghoff, *Ambiguities in State Security Breach Notification Statutes, in* DATA BREACH AND ENCRYPTION HANDBOOK 89, 94–97 (Lucy Thompson ed., 2011) (discussing the various definitions for "encryption" used in data breach notification statutes).

47. *Riley*, 134 S. Ct. at 2486.

48. *Id.*

confronted with a 'now or never' situation . . . they may be able to rely on exigent circumstances to search the phone immediately," rather than invoking the exception for searches incident to arrest.[49]

The Court also justified its departure from *Robinson*'s categorical rule based on the unique nature of cell phones, which "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[50] In particular, the Court emphasized the "immense storage capacity" of modern cell phones and "many distinct types of information" that can be stored therein, making it possible to reconstruct "[t]he sum of an individual's private life."[51] The Court also recognized that data stored on cell phones, including internet browsing history, historical location data, and mobile apps, is qualitatively different from physical records.[52] Based on these facts, the *Riley* Court concluded that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."[53]

Although the government conceded that the search incident to arrest doctrine would not extend to a search of files accessed remotely, the Court briefly discussed the complications presented by cloud computing technology in determining the scope of an individual's privacy interests.[54] The Court was skeptical of the cell phone-as-container comparison, and found that "the analogy crumbles entirely when a cell phone is used to access data located elsewhere."[55] Thus, in *Riley*, the Court recognized the unique privacy considerations attendant to searches of digital devices, as compared to physical searches.

C. The Private Search Doctrine

In *Burdeau v. McDowell*, the Court clearly established that the Fourth Amendment does not apply to the conduct of private individuals.[56] The Court found that the Fourth Amendment's "origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies[.]"[57]

49. *Id.* at 2487 (internal quotation marks omitted) (quoting Missouri v. McNeely, 133 S. Ct. 1552, 1561 (2013)).

50. *See id.* at 2489.

51. *Id.*

52. *Riley*, 134 S. Ct. at 2490.

53. *Id.* at 2491.

54. *Id.*

55. *Id.*

56. 256 U.S. 465, 475 (1921).

57. *Id.*

Based upon this Fourth Amendment requirement of "governmental action," the Court recognized the private search doctrine,[58] under which "government examination of an object that merely replicates a previous private search is not a 'search' within the meaning of the Fourth Amendment; rather, the Amendment applies only to the extent that the government has exceeded the scope of the private search."[59]

The application of the private search doctrine generally centers on two main issues: establishing that the initial search was conducted by a private actor, and determining the permissible scope of the secondary government search.[60] While it is well established that a search or seizure initiated by a private party is not prohibited by the Fourth Amendment, the conduct of a private actor may be considered state action in some circumstances.[61] "Whether a private party should be deemed an agent or instrument of the Government for *Fourth Amendment* purposes necessarily turns on the degree of the Government's participation in the private party's activities . . . in light of all the circumstances."[62] In making this determination, courts have considered "1) whether the Government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[63]

The second issue, which the Court addressed in *United States v. Jacobsen*, concerns whether the secondary government search properly replicated the initial private search.[64] In that case, FedEx employees opened a damaged package for inspection, pursuant to the company policy for insurance claims.[65] The box contained a ten-inch tube, which was taped closed and nestled inside crumpled newspaper.[66] A supervisor cut open the tube and found zip-lock plastic bags containing white powder.[67] After contacting the Drug Enforcement Administration (DEA),

58. *Id.* at 475.

59. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 331 (2008).

60. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114–15 (1983).

61. PRISCILLA GRANTHAM ADAMS, FOURTH AMENDMENT APPLICABILITY: PRIVATE SEARCHES 2 (2008).

62. Skinner v. Ry. Labor Execs'. Ass'n, 489 U.S. 602, 614 (1989) (internal quotations marks omitted) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

63. United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000) (quoting Pleasant v. Lovell, 876 F.2d 787, 797 (10th Cir. 1989)); *see* United States v. Jarrett, 338 F.3d 339, 345 (4th Cir. 2003); United States v. Grimes, 244 F.3d 375, 383 (5th Cir. 2001).

64. 466 U.S. at 111.

65. *Id.* at 111.

66. *Id.*

67. *Id.*

the FedEx employees placed the bags, tube, and newspaper back into the box in the same manner as they had been discovered.[68] When the first DEA agent arrived,

> [T]he box [was] still wrapped in brown paper, but with a hole punched in its side and the top open, was placed on a desk. The agent saw that one end of the tube had been slit open; he removed the four plastic bags from the tube and saw the white powder. He then opened each of the four bags and removed a trace of the white substance with a knife blade. A field test made on the spot identified the substance as cocaine.[69]

At issue in *Jacobsen* was whether the DEA agent's testing of the powder was a "search" within the scope of the Fourth Amendment, such that a warrant was required.[70] The Court found that "[t]he additional invasions of . . . privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search."[71]

In *Walter v. United States*, a case previously decided by the U.S. Court of Appeals for the Fifth Circuit, a plurality of justices agreed that the legality of the secondary government search should be evaluated in light of the extent of the private search.[72] The seven–two majority in *Jacobsen* adopted this approach, finding it consistent with "the analysis applicable when private parties reveal other kinds of private information to the authorities," such as the third-party doctrine.[73]

Ultimately, the *Jacobsen* Court determined "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct."[74] "Even if the white powder was not itself in 'plain view' because it was still enclosed . . . there was a *virtual certainty* . . . that a manual inspection of the tube and its contents would not tell [the DEA agent] anything more than he already had been told."[75] With respect to the violation of respondent's possessory interest in the white powder during the field test, the Court concluded that the infringement was de minimis and reasonable in light of the substantial law enforcement interests.[76] Thus, following *Jacobsen*, the test for whether an individual's privacy right has been compromised—permitting a warrantless government search under the

68. *Id.*
69. *Jacobsen*, 466 U.S at 111–12.
70. *Id.* at 112.
71. *Id.* at 115.
72. *See* 447 U.S. 649, 652, 657 (1980) (plurality opinion).
73. *See Jacobsen*, 466 U.S. at 117.
74. *Id.* at 126.
75. *Id.* at 118–19 (emphasis added).
76. *See id.* at 125.

private search doctrine—is whether the government actors are "virtually certain" of what they will find.[77] However, given the tremendous rate of technological innovation and widespread adoption of the internet in the three decades since *Jacobsen* was decided, courts have struggled to define the scope of the private search doctrine in the digital age.

II. CLOUD STORAGE TECHNOLOGY AND DIGITAL FORENSICS

Whether we realized it or not, cloud computing has become ubiquitous in the modern age, gaining popularity among both business and personal users. Cloud computing permits access to remotely-located computer resources through the internet or an internal network, in contrast to traditional mainframe computing, where in-house servers generate computing power to run programs and store information.[78] According to Cisco's Global Cloud Index, cloud data centers will account for eighty-eight percent of global data storage capacity by 2020.[79] With regard to individual use of cloud storage, Cisco estimates that "[b]y 2020, 59 percent (2.3 billion) of the [worldwide] consumer Internet population will use personal cloud storage, up from 47 percent (1.3 billion users) in 2015."[80] Moreover, the amount of data used by consumers in cloud storage is projected to reach 1.7 gigabytes per month by 2020, a three-fold increase from 2015.[81]

The National Institute of Standards and Technology defines cloud computing as "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) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[82] This definition includes a wide variety of products, all of which share five essential characteristics: (1) on-demand self-service; (2) broad network access; (3) resource pooling; (4) rapid elasticity; and (5) measured service.[83]

77. *See id.* at 19.

78. Quick & Choo, *supra* note 3, at 266; *see* William Voorsluys, James Broberg & Rajkumar Buyya, *Introduction to Cloud Computing*, *in* CLOUD COMPUTING: PRINCIPLES AND PARADIGMS 3, 5 (Rajkumar Buyya et al. eds., 2011).

79. CISCO PUB., CISCO GLOBAL CLOUD INDEX: FORECAST AND METHODOLOGY 2015–2020, at 3 (2016), https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf.

80. *Id.* at 3.

81. *Id.*

82. PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

83. *Id.*

Cloud computing services can be categorized based upon the types of user capabilities provided and the service models of the providers. At the bottom level of cloud computing systems is "Infrastructure as a Service" (IaaS).[84] IaaS provides "processing, storage, networks, and other fundamental computing resources," upon which the consumer can run software.[85] Other cloud services, described as "Platform as a Service" (PaaS), offers consumers an easily-programmable environment, with the option to deploy applications using "programming languages, libraries, services, and tools supported by the provider."[86] At the most sophisticated and user-friendly level is "Software as a Service" (SaaS), which allows consumers "to use the provider's applications running on a cloud infrastructure."[87] The consumer can access the applications through a "thin client interface, such as a web browser (e.g., web-based email), or a program interface."[88]

A. The Mechanics of Cloud Storage

Generally, commercial cloud storage is IaaS, by which the provider offers the consumer access to computer servers and data storage.[89] Consumer offerings, like Dropbox, Google Drive, iCloud, and Microsoft OneDrive, are SaaS, providing both the storage space and the software to utilize it.[90] However, the unifying feature of both offerings is that the stored data is not "local"—that is, the information may be contained in data pools in a server miles (or thousands of miles) away.[91] Through application programming interfaces ("API"), like web-based content management systems or desktop applications, users have instant access to this remotely-stored data.[92] For desktop applications, the cloud-stored files appear "mirrored" on the user's computer, but the data is not stored

84. Voorsluys et al., *supra* note 78, at 13–14 (citing Daniel Nurmi et al., *The Eucalyptus Open-source Cloud-computing System*, *in* 9TH IEEE/ACM INTERNATIONAL SYMPOSIUM ON CLUSTER COMPUTING AND THE GRID 124–31 (Franck Cappello et al. eds., 2009)).

85. MELL & GRANCE, *supra* note 82, at 3.

86. *Id.* at 2–3; Voorsluys et al., *supra* note 78, at 14.

87. MELL & GRANCE, *supra* note 82, at 2.

88. *Id.*

89. *See* Voorsluys et al., *supra* note 78, at 13–14 (citing Borja Sotomayor et al., *Virtual Infrastructure Management in Private and Hybrid Clouds*, 13 IEEE INTERNET COMPUTING 14, 14–22 (2009)).

90. Quick & Choo, *supra* note 3, at 266.

91. *See* Quentin Hardy, *Where Does Cloud Storage Really Reside? And Is It Secure?*, N.Y. TIMES (Jan. 23, 2017), https://www.nytimes.com/2017/01/23/insider/where-does-cloud-storage-really-reside-and-is-it-secure.html.

92. *See* OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK 831 (Adam Gordon ed., 4th ed. 2015).

on the hard drive of the accessing computer.[93]

Another important feature of cloud storage is its "multi-tenancy capability."[94] Multi-tenancy is the "ability of cloud services to support use of the same resources or applications by multiple users," permitting simultaneous multi-point, multi-user access.[95] On the other hand, "[u]nder certain circumstances, individual files from individual customers may be distributed across multiple disks and storage systems across multiple jurisdictions if a cloud service provider (CSP) has facilities in more than one country."[96]

B. Data Recovery and Chain of Custody Issues

The unique structure of cloud systems presents significant challenges to law enforcement investigations. In the past, digital forensic tools relied "upon having physical access to the media that stores the data of potential interest."[97] In contrast to physical hard drives, which police can easily seize, "clone," and examine; securing data in the cloud is comparatively difficult.

First, physical seizure of the servers may be complex, or impossible, due to the intrinsic features of cloud computing. Servers are often located overseas, creating jurisdictional issues.[98] Furthermore, "data distribution technologies may split a user's data across a number (potentially thousands) of storage devices within the cloud computing environment."[99]

Second, some cloud systems do not have the capability to preserve the data in the manner required by investigators.[100] Before exporting the information, the data must be preserved to ensure that potential evidence is not altered.[101] Because this function is not supported by all cloud environments, there is the potential for "accidental modification of data as it is exported from the cloud computing environment for [law enforcement] use or intentional destruction of data by the suspect."[102]

Finally, once the data is exported, it may be difficult for law

93. *See generally id.* (explaining cloud and virtual data storage models compared to physical data storage).

94. QUICK, MARTINI & CHOO, *supra* note 7, at 5.

95. *Id.*

96. *Id.*

97. *Id.* at 6.

98. *Id.*

99. QUICK, MARTINI & CHOO, *supra* note 7, at 6.

100. *Id.* at 7.

101. *Id.*

102. *Id.*

enforcement to analyze.[103] Despite the increasingly common use of cloud systems, "most of the prevalent digital forensic analysis tools have not yet been updated to decode the major cloud computing data export formats."[104]

The strengths of cloud computing as a service to consumers often create challenges to law enforcement investigations.[105] While the multi-tenancy capability of cloud systems is a critical feature of the service, it has the potential to raise serious privacy concerns. Since cloud services can support the use of the same resources by multiple users, a government search of a cloud storage server may expose the information of many individuals.[106]

III. THE SCOPE OF GOVERNMENT SEARCHES OF DIGITAL DEVICES UNDER THE PRIVATE SEARCH DOCTRINE

A. The "Disk-Based" Approach

The "disk-based" theory posits that even a non-comprehensive private search of the files contained within a digital device will permit a secondary government search of all data on the device. This approach was first articulated by the Fifth Circuit in *United States v. Runyan*.[107] In that case, Runyan was convicted of sexual exploitation of children and of possession and distribution of child pornography based on images contained in Polaroid photos, 3.5 inch floppy discs, CD's, ZIP disks, and a desktop computer.[108] The materials were discovered by Runyan's ex-wife and friends, at the time she moved out of their shared home.[109] After viewing some of the disks and determining that they contained child pornography, all of the materials were turned over to law enforcement.[110] On appeal, Runyan argued that the trial court erred in refusing to suppress evidence directly and indirectly stemming from pre-warrant searches of

103. *Id.*

104. QUICK, MARTINI & CHOO, *supra* note 7, at 7.

105. George Grispos, Tim Storer & William Bradley Glisson, *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*, 4 INT'L J. OF DIGITAL CRIME & FORENSICS 28, 29 (2012).

106. *See* Larry Bourgeois, *What is Multi-Tenancy? How Secure is It?*, ASIGRA BLOG (Mar. 9, 2011), http://www.asigra.com/blog/what-multi-tenancy-how-secure-it; Wayne J. Brown, Vince Anderson & Qing Tan, *Multitenancy – Security Risks and Countermeasures*, *in* 15TH INTERNATIONAL CONFERENCE ON NETWORK-BASED INFORMATION SYSTEMS 7, 7–8 (2012).

107. *See* 275 F.3d. 449, 465 (5th Cir. 2001) (holding that a police search of Runyan's computer was permitted even though it was more intrusive that the initial private search).

108. *Id.* at 452–53.

109. *Id.*

110. *Id.* at 453.

the disks by federal and state law enforcement.[111] He contended that because the police officers examined more of the disks, looked at more of the images on each disk, and printed out selected images contained on the disks, the government search "exceeded the scope" of the initial private search.[112]

Regarding the search of digital materials, the court distinguished three narrow inquiries into the proper scope of a secondary government search.[113] As an initial matter, the court addressed "whether a police search exceeds the scope of a private search when private searchers examine selected items from a collection of similar closed containers and police searchers subsequently examine the entire collection."[114] The court noted language in *Jacobsen* supporting the proposition that "confirmation of prior knowledge does not constitute exceeding the scope of a private search," as such an expansion "frustrates no expectation of privacy that has not already been frustrated."[115] Based on this rationale, the Fifth Circuit determined that even when a closed container was not examined during the initial private search, police do not exceed the scope of that search by opening the container when they "are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise."[116] Applied to the present case, the court held "that the police's pre-warrant examination of the disks clearly exceeded the scope of the private search" as they could not have had "substantial certainty" that all of the disks contained child pornography.[117] Therefore, the disks and any evidence derived from the police search could be subject to suppression.[118]

Subsequently, the court considered "whether a police search exceeds the scope of the private search when the police examine more items within a particular container than did the private searchers."[119] The Fifth Circuit determined that "it would not have been constitutionally problematic for the police to have examined more files than did the private searchers."[120] The court found that because an individual's

111. *Id.* at 456.
112. *Runyan*, 275 F.3d at 460.
113. *Id.* at 461–62.
114. *Id.*
115. *Id.* at 463.
116. *Id.*
117. *Runyan*, 275 F.3d at 464.
118. *Id.*
119. *Id.* at 461.
120. *Id.* at 464.

expectation of privacy in the contents of a container is compromised once the container is opened and examined during a private search, "the police do not engage in a new 'search' for Fourth Amendment purposes each time they examine a particular item found within the container."[121] Thus, applied to Runyan's case, the Fifth Circuit determined "that the police in the instant case did not exceed the scope of the private search if they examined more files on the privately-searched disks" than the initial private searchers, and suppression of such files was unnecessary.[122]

Eleven years later, the Seventh Circuit adopted the same rules in *Rann v. Atchinson*.[123] In that case, Rann was convicted of criminal sexual assault and possession of child pornography, based on digital images obtained from a camera memory card and ZIP drive without a warrant.[124] The memory card had been given to police by Rann's daughter, who was one of his victims, and the ZIP drive had been obtained and taken to police by the girl's mother.[125] Rann appealed his conviction, contending that he received ineffective assistance of counsel because his attorney failed to seek suppression of the images recovered from the drives.[126]

The Seventh Circuit concluded that Rann's suppression claim was without merit, as the secondary government search did not violate the Fourth Amendment.[127] In doing so, the court applied both of the Fifth Circuit's rules from *Runyan*.[128] With regard to disks that had been examined by a private searcher, the court agreed that a subsequent police search would be "valid if the private party who conducted the initial search had viewed at least one file on the disk."[129] Furthermore, even if a disk had not been examined by the private searcher, the police would not be found to have exceeded the scope of the private search if they were "substantially certain of what [was] inside the container."[130] The court found that these rules "strike[] the proper balance between the legitimate expectation of privacy an individual retains in the contents of his digital media storage devices after a private search has been conducted and the additional invasion of privacy" that occurs during a government search

121. *Id.* at 465.
122. *Runyan*, 275 F.3d at 465.
123. 689 F.3d 832, 837 (7th Cir. 2012).
124. *Id.* at 833–34.
125. *Id.* at 834.
126. *Id.* at 833.
127. *Id.* at 838.
128. *See Rann*, 689 F.3d at 836–37.
129. *Id.* at 836 (citing United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001)).
130. *Id.* at 836–37 (quoting *Runyan*, 275 F.3d. at 463).

which exceeds the scope of the initial private search.[131] Applied in the instant case, the court determined that the private actors "knew the contents of the digital media devices when they delivered them to the police" and therefore the police were "substantially certain" that the devices contained child pornography, justifying a comprehensive search of the drives under either rule.[132]

B. The "Data-Based" Approach

In contrast, the narrower "data-based" approach limits the secondary government search to the actual data or files accessed by the initial private searcher. This approach was applied by the Sixth Circuit in *United States v. Lichtenberger*.[133] In *Lichtenberger*, the defendant successfully suppressed evidence of child pornography that was found on his laptop computer, and the government appealed.[134] The materials were discovered by Lichtenberger's girlfriend, Karley Holmes, who had hacked into his laptop after learning that he had been previously convicted of child pornography offenses.[135] After observing several folders containing thumbnail images of child pornography, Holmes closed the computer and contacted the police.[136] The responding officer asked her to boot up the computer and show the images to him, and Holmes opened several folders and "click[ed] on random thumbnail images to show him."[137] Later, Holmes testified that she had seen approximately one hundred images during her initial search, and that some of the images she showed to the officer came from the same file, but she was uncertain as to whether they were ones she had previously viewed.[138] The officer asked Holmes to retrieve other electronic devices, including Lichtenberger's cell phone and flash drive, which he took back to the station along with the laptop.[139] On appeal, the government argued that the officer's review and subsequent seizure of the laptop was permissible under the private search doctrine.[140]

While it ultimately agreed with the district court's conclusion, the

131. *Id.* at 837 (internal quotation marks omitted) (quoting United States v. Jacobson, 466 U.S. 109, 115 (1983)).

132. *Id.* at 838 (citing *Runyan*, 275 F.3d. at 463).

133. *See* 786 F.3d 478, 491 (6th Cir. 2015).

134. *Id.* at 480.

135. *Id.*

136. *Id.*

137. *Id.*

138. *Lichtenberger*, 786 F.3d at 481.

139. *Id.*

140. *Id.* at 481.

Sixth Circuit determined that the lower court erred in deciding the issue on agency grounds, rather than first comparing the scope of the two searches.[141] The Sixth Circuit emphasized *Jacobsen*'s "virtual certainty" requirement, which it related to the heightened privacy interests in cell phones and digital devices, which the Supreme Court recognized in *Riley*.[142] Returning to Fourth Amendment fundamentals, the court stated, "we must weigh the government's interest in conducting the search of Lichtenberger's property against his privacy interest in that property . . . under *Riley*, the nature of the electronic device greatly increases the potential privacy interests at stake, adding weight to one side of the scale."[143]

In *Lichtenberger*, the Sixth Circuit read the *Jacobsen* scope test narrowly, and determined that there was "no virtual certainty that [the officer's] review was limited to the photographs from Holmes's earlier search[,]" and that the officer could have exceeded the scope of the initial search.[144] Moreover, it was possible that the officer "could have discovered something else on Lichtenberger's laptop that was private, legal, and unrelated to the allegations," which was exactly what the Supreme Court sought to prevent through its "beyond-the-scope" test.[145] The Sixth Circuit noted that given the "reality of modern data storage . . . the possibilities [of finding unrelated information] are expansive."[146]

Within the same year that the Sixth Circuit decided *Lichtenberge*r, the Eleventh Circuit likewise adopted a "data-based" theory of scope in resolving a private search doctrine question in *United States v. Johnson*.[147] In *Johnson*, the defendants appealed the denial of their motion to suppress child pornography, which was recovered during a warrantless search of their cell phone, subsequent to an initial private search.[148] After Sparks' phone was accidentally left at a Walmart, it was subsequently found by a store employee, with whom she arranged the

141. *Id.* at 484–85 ("[A]gency is relevant to an after-occurring search analysis where the court determines that the after-occurring search exceeds the scope of the initial private search.").

142. *Id.* at 488; Riley v. California, 134 S. Ct. 2473, 2493 (2014); United States v. Jacobsen, 466 U.S. 109, 119 (1983).

143. *Lichtenberger*, 786 F.3d at 488.

144. *Id.*

145. *Id.* at 488–89.

146. *Id.* at 489.

147. *See generally* 806 F.3d 1323 (11th Cir. 2015) (deciding it was appropriate to consider the data and contents of the defendant's mobile phone, and what of those contents law enforcement had seen in resolving a private search doctrine issue).

148. *Id.* at 1330.

return of the device.[149] Prior to returning the phone, the employee examined the contents of the phone's digital photo album and discovered that it contained "questionable" images that could be child pornography.[150] The employee consulted her fiancé, David Widner, to decide what to do, showing him several images and describing a video that she had seen on the phone.[151] Together, they scrolled through a number of thumbnail images contained in a digital album, and examined several full-size images.[152] Widner then brought the phone to the police department to file a report about the images, which he believed to be child pornography.[153] With the police officers observing, Widner scrolled through the phone to identify the images that concerned him, viewing the album in thumbnail form and stopping to display specific images in full-size.[154] The phone was then given to Detective-Sergeant Brian O'Reilly, who looked at the photos in the phone album and also viewed a video saved on the phone, which Widner had not watched.[155] A search warrant for Sparks' residence was issued on the basis of an affidavit that included O'Reilly's descriptions of the material he had seen on the phone.[156]

On appeal, the defendants argued the cell phone photos, videos, and other materials recovered during a search of their home should be suppressed because the District Court erred in "finding that the warrantless search of the cell phone by [the police] did not exceed the scope of the [private] search."[157] The Eleventh Circuit agreed that O'Reilly's secondary search of the cell phone, specifically his viewing of a video that Widner had not seen, exceeded the scope of the initial private search.[158] With regard to the materials that Widner had examined, the court noted that "[t]hough O'Reilly may have looked at some of the photos and the video more closely than did Widner . . . the private party's earlier viewing of the same images and video insulated law enforcement's later, more thorough review of them from transgressing the Fourth Amendment."[159] However, when O'Reilly viewed the second video, this government search "exceeded—not replicated—the breadth of the

149. *Id.* at 1329.
150. *Id.* at 1330.
151. *Id.* n.4.
152. *Johnson*, 806 F.3d at 1331.
153. *Id.*
154. *Id.*
155. *Id.* at 1331–32.
156. *Id.* at 1332–33.
157. *Johnson*, 806 F.3d at 1333.
158. *Id.* at 1335.
159. *Id.* at 1336.

private search."[160] Citing the Supreme Court's decision in *Riley*, the court concluded that "[w]hile Widner's private search of the cell phone might have removed certain information from the Fourth Amendment's protections, it did not expose every part of the information contained in the cell phone."[161] Nevertheless, the court determined that the error had no effect on the validity of the warrants, which were supported by other evidence constituting probable cause, and affirmed the District Court's judgment.[162]

IV. APPLICATION OF THE "DISK-BASED" AND "DATA-BASED" APPROACHES TO THE CLOUD STORAGE CONTEXT

As consumers increasingly turn to cloud storage for convenience and security, it is critical that the government respects the significant privacy interests associated with cloud-stored data and cloud-connected devices. Both the "disk-based" and "data-based" approaches to the private search doctrine attempt to circumscribe the scope of a permissible search under the Fourth Amendment. As illustrated in the cases above, the lower courts addressing this issue consistently return to Fourth Amendment fundamentals, weighing the degree of intrusion into an individual's privacy interest against the promotion of legitimate government interests.

However, in the cloud storage context, the "disk-based" approach to defining the scope of a search is untenable. While this bright-line rule is easy to administer with respect to locally-stored data, the cloud has unique features which present issues not adequately addressed by the "disk-based" approach. First, the container analogy upon which the "disk-based" approach is premised no longer works when considering remotely-stored data. Second, the unlimited storage capacity and flexibility of cloud storage allow it to be used for many purposes, making it less likely that government agents can be "virtually certain" of what a cloud drive contains.

By merely looking at a cloud-connected device, it is impossible to know the nature or quantity of information accessible through it, defeating the analogy to a closed container. Unlike traditional hard drives or local servers, data in the cloud is not confined to any single, identifiable device—by its design, it exists throughout a network of connected data pools. This infinitely scalable structure permits cloud storage to be used for files of any size. In contrast, a closed container is limited to its

160. *Id.*

161. *Id.* (citing Riley v. California, 134 S. Ct. 2473, 2489 (2014)).

162. *Johnson*, 806 F.3d at 1336.

physical dimensions. Based on its shape alone, government agents can gain some insight into its contents and estimate the maximum size of what might be contained inside. As the Court noted in *Riley*, digitally stored information is both quantitatively and qualitatively different from physical evidence.[163] In the cloud context, the Court's concerns regarding "immense storage capacity" and "distinct types of information" saved therein are exponentially magnified.[164]

Due to the flexibility of cloud storage and the public's increasing reliance on this technology, a single user may use cloud storage for any number of diverse purposes. In such cases, it is unlikely that government agents can be "virtually certain" of what they will find within a single cloud drive, if the initial private search was not comprehensive.[165] In *Runyan*, the Fifth Circuit's application of the "disk-based" approach was premised on the idea that government actors could be "substantially certain of what is inside the container" based on the statements of the private searchers and their expertise.[166] However, the unique features and capabilities of cloud storage technology weaken this assumption. Even within a single account, cloud storage may be utilized for any number of distinct purposes, including storage of business, educational, or personal documents. Unlike a CD or flash drive, which can contain only a limited amount of data, cloud storage has an infinite capacity—enabling the centralized storage of almost all digital information relevant to a person's life. During a secondary search of a cloud-linked device, the secondary government searchers are unlikely to have "virtual certainty" regarding its contents, failing the standard articulated in *Jacobsen*.

Furthermore, from a public policy perspective, the "disk-based" approach may ultimately become tremendously burdensome on government investigations. Under the "disk-based" theory of scope, the government would be required to establish that the initial private search included at least some data from every remotely-located cloud server that was examined in the secondary government search. Moreover, this approach would theoretically expose all of the data on a remote server, which is likely to include significant amounts information irrelevant to the government's investigation or saved by other individuals. In contrast, the "data-based" approach to scope properly protects individual privacy interests, even in a cloud context. The "data-based" rule encourages use of the warrant process and judicial oversight. Although the "data-based"

163. *Riley*, 134 S. Ct. at 2489.

164. *Id*.

165. United States v. Jacobsen, 466 U.S 109, 125 (1983).

166. United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001).

approach limits the information immediately accessible to government actors, the Court was unconvinced by a similar argument for permitting cell phone searches in *Riley*.[167] Similar risks of data destruction and encryption exist in the cloud storage context, but do not justify extensive intrusions into personal privacy.

Additionally, the "data-based" approach to scope within the private search doctrine is consistent with precedent in the Tenth Circuit, where it found that an individual file was the relevant unit of a search, in considering the government's argument under the Fourth Amendment's plain view doctrine.[168] The court noted that "law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[169] Similar techniques are possible and permissible in the cloud context, provided that a warrant is obtained. The "data-based" approach to scope applies to permit a secondary government examination, but does not foreclose the police from using the information provided by a private actor to obtain a warrant for more thorough examination.

CONCLUSION

Given the significant privacy interests present in digital devices, as recognized by the Supreme Court in *Riley*, the scope of permissible searches under the private search doctrine should be narrowly construed. This position finds even greater support when considering secondary government searches of cloud storage, which have greater storage capacity than the cell phones considered in *Riley* and can similarly be used to store many kinds of information. Therefore, the "data-based" theory of scope is best suited for application to searches of cloud-stored information, which presents unique challenges to the traditional Fourth Amendment analysis. Under this model, the government will be able to obtain the benefit of the data viewed by a private actor, but is restricted from wholesale rummaging. Following this narrowly-construed secondary search, the government is likely to have sufficient information to procure a warrant, if necessary. Such a rule is consistent with Fourth Amendment precedent and properly balances individual privacy interests against the government's law enforcement objectives.

167. *Riley*, 134 S. Ct. at 2487.

168. United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999).

169. *Id.* at 1276 (citing Winick, *supra* note 30, at 107).