Denver Law Review

Volume 94 | Issue 4 Article 7

January 2017

You've Got Mail: Decoding the Bits and Bytes of Fourth Amendment Computer Searches after Ackerman

Roderick O'Dorisio

Follow this and additional works at: https://digitalcommons.du.edu/dlr

Recommended Citation
Roderick O'Dorisio, You've Got Mail: Decoding the Bits and Bytes of Fourth Amendment Computer Searches after Ackerman, 94 Denv. L. Rev. 651 (2017).

This Note is brought to you for free and open access by the Denver Law Review at Digital Commons @ DU. It has been accepted for inclusion in Denver Law Review by an authorized editor of Digital Commons @ DU. For more information, please contact jennifer.cox@du.edu,dig-commons@du.edu.

You've Got Mail: Decoding the Bits and Bytes of Fourth Amendment Computer Searches after Ackerman

This note is available in Denver Law Review: https://digitalcommons.du.edu/dlr/vol94/iss4/7

"YOU'VE GOT MAIL!" DECODING THE BITS AND BYTES OF FOURTH AMENDMENT COMPUTER SEARCHES AFTER *ACKERMAN*

ABSTRACT

In the digital age, courts have been searching for rational solutions and definitions regarding computer searches that comport with current Fourth Amendment law, specifically the private search doctrine. Recently, in *United States v. Ackerman*, the U.S. Court of Appeals for the Tenth Circuit held that when a government entity or agent opens and examines emails previously unopened by private actors, they have conducted a "search" to which the Fourth Amendment applies. Although the ultimate holding is consistent with the Fourth Amendment's reasonable expectation of privacy doctrine, the Tenth Circuit offered a controversial alternative rationale rooted in the trespass-to-chattels doctrine. This alternative rationale has far-reaching implications, specifically regarding the viability of the private search doctrine as applied to computer searches.

This Comment first argues that courts should adopt a "file" approach in Fourth Amendment cases involving searches of computers rather than the previously proposed "physical device" and "human observation" approaches. A person who leaves a file open on a computer does not possess a reasonable expectation of privacy in the open file, but a person does possess a reasonable expectation of privacy in closed files. Secondly, this Comment argues that the reintroduction of the trespass-to-chattels limb of Fourth Amendment searches will practically extinguish the private search doctrine as applied to computers, unless courts adopt a different definition of "trespass," specifically a definition anchored in the unit of a computer file. The abstract concept of a computer file is analogous to the "metes and bounds" of physical property, and the data contained within the file is analogous to the property contained within said physical metes and bounds. Under both the reasonable expectation of privacy and trespass-to-chattels doctrines, focusing on the unit of a computer "file" is the most favorable approach. In short, opening a file on a computer should be considered a distinct search under the Fourth Amendment and therefore should require a distinct justification.

TABLE OF CONTENTS

INTRODUCTION

As technology continues to rapidly advance and become more integrated in our day-to-day lives, computer evidence will increasingly become more valuable and pertinent in both civil and criminal investigations. Computer forensic examination is now a common tool in almost all criminal investigations.[1] To support this tool, the Federal Bureau of Investigation (FBI) alone has over two hundred full-time computer forensic examiners.[2] However, computer forensic examination continues to generate unnecessary Fourth Amendment complications. Because most modern-day computers possess storage capacities from anywhere between 250 gigabytes to several terabytes,[3] the application of the Fourth Amendment becomes problematic. In light of their "immense storage capacit[ies]"[4] and ability to store and transport "millions of pages of text, thousands of pictures, or hundreds of videos,"[5] electronic devices are quantitatively different from physical spaces. Electronic records, unlike physical records, possess an "element of pervasiveness" because electronic records can be transferred among devices around the world in milliseconds whereas physical records cannot.[6] Furthermore, electronic de-

1. Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 112 (2011).

2. U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION 131 (2010).

3. *See* Kim Komando, *How Much Computer Storage Do You Really Need?*, USA TODAY (Nov. 30, 2012, 7:51 AM), http://www.usatoday.com/story/tech/columnist/komando/2012/11/30/komando-computer-storage/1726835; Lucas Mearian, *With Tech Breakthrough, Seagate Promises 60TB Drives this Decade*, COMPUTERWORLD (Mar. 20, 2012, 11:58 AM), https://www.computerworld.com/article/2502838/data-center/with-tech-breakthrough--seagate-promises-60tb-drives-this-decade.html.

4. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014).

5. *See id.*

6. *Id.* at 2490 ("[A]n element of pervasiveness characterizes cell phones but not physical records.").

vices are qualitatively different than physical spaces because data stored on electronic devices may include "private information never found in a home in any form."[7] For example, consider an electronic device's persistent tracking of Global Positioning System (GPS) location data or artificial intelligence algorithms that determine a user's social profile and preferences. Such private information rarely exists in physical form in a home because displaying this information on a tangible medium requires printing tens of thousands of pages.[8]

The Fourth Amendment is heavily premised on physical objects and was drafted to regulate searches of homes and physical property.[9] Until the Warren Court, judicial interpretation of the Fourth Amendment protected only against physical intrusions on tangible things.[10] This purely physical conception of the Fourth Amendment's protections changed with the seminal decision of *Katz v. United States*,[11] where the Court replaced property-based theories with a two-part "expectation of privacy" test.[12] According to *Katz*, a search under the Fourth Amendment occurs when a governmental employee or agent of the government violates an individual's reasonable expectation of privacy.[13] However, because the Fourth Amendment applies only to governmental employees and agents, the Fourth Amendment is not triggered when private parties conduct searches.[14] The Supreme Court established the "private search doctrine" to regulate what law enforcement is allowed to see without complying with the strictures of the Fourth Amendment.[15] The private search doctrine allows police and law enforcement officials to reconstruct the private party search and see what the private party saw, but police and

7. *Id.* at 2491.

8. 1.4 gigabytes (GB) is equivalent to 105,000 pages. 5.8 GB is equivalent to 435,000 pages. 5,200 GB is equivalent to 390,000,000 pages. *See Data Volume Estimates and Conversions*, SDS DISCOVERY, http://www.sdsdiscovery.com/resources/data-conversions (last visited May 30, 2017); *see also* ERICSSON, ERICSSON MOBILITY REPORT: ON THE PULSE OF THE NETWORKED SOCIETY 2 (2016) (total monthly mobile data traffic per smartphone was 1.4 GB in 2015; total monthly mobile data traffic per mobile PC was 5.8 GB in 2015); *see also* International Data Corporation, *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East*, EMC (Dec. 2012), https://www.emc.com/leadership/digital-universe/2012iview/executive-summary-a-universe-of.htm (the digital universe will exceed 40 trillion GB, which is "5,200 GB for every man, woman, and child").

9. *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 290–92 (2005).

10. Olmstead v. United States, 277 U.S. 438, 466 (1928) (noting that no precedents permit the Fourth Amendment to apply as a viable defense in cases where no official search and seizure of the person, his papers, tangible material effects, or an actual physical invasion of property had occurred), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

11. 389 U.S. 347 (1967).

12. *Id.* at 353.

13. *Id.* at 360–61 (Harlan, J., concurring) (articulating the test commonly associated with *Katz*); *see also* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

14. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

15. *Id.* at 115–16.

law enforcement may not exceed the scope of the private party search without triggering the Fourth Amendment.[16] A private search extinguishes an individual's reasonable expectation of privacy in the object searched;[17] once this has occurred, the Fourth Amendment does not prohibit governmental use of this non-private information.[18] By merely repeating the search, the government does not further infringe on a person's privacy.[19] Unsurprisingly, the private search doctrine's application to electronic devices has caused controversy within federal courts.[20]

Although this privacy rationale has been the touchstone of Fourth Amendment searches for almost fifty years, in 2012, *United States v. Jones*[21] supplemented the reasonable expectation of privacy doctrine by reintroducing the trespass doctrine.[22] If an individual does not have a reasonable expectation of privacy, a governmental employee or agent may still trigger a Fourth Amendment "search" by trespassing onto that individual's property in order to obtain information.[23] With regard to the private search doctrine, even though a police officer accurately repeated a prior private search, the police officer's repeated search would qualify as a "trespass" under *Jones* and therefore a distinct search under the Fourth Amendment. Thus, the prior private party search becomes irrelevant under a *Jones* trespass-to-chattels analysis, which inevitably challenges the continued viability of the private search doctrine as applied to computers.[24]

This Comment explores both the history and future of Fourth Amendment computer searches in light of the Tenth Circuit's recent ruling in *United States v. Ackerman*[25] and concludes by proposing a simple framework for administering the Fourth Amendment that preserves the private search doctrine regarding computers. This Comment will argue that by adopting a "file" framework for defining computer searches, both

16. *Id.* at 115–20.
17. *Id.* at 117.
18. *Id.*
19. *Id.* at 120.
20. *Compare* United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001) (holding that police did not exceed the scope of the private party's search by opening and viewing additional files on CDs), *and* Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012) (holding that police did not exceed scope of the private party's search after opening and searching previously unopened files on a zip drive), *with* United States v. Lichtenberger (*Lichtenberger II*), 786 F.3d 478, 491 (6th Cir. 2015) (holding that police exceeded the scope of the private party's search when files were opened on the same device that had not been searched earlier), *and* United States v. Sparks, 806 F.3d 1323, 1335 (11th Cir. 2015) (holding that police exceeded the scope of the private party's search when previously unopened images and a video were searched on the same device).
21. 565 U.S. 400 (2012).
22. *Id.* at 405–06 (citing Olmstead v. United States, 277 U.S. 438 (1928)) (discussing the trespass rule).
23. *Id.* at 407–08.
24. *See, e.g.*, Andrew MacKie-Mason, *The Private Search Doctrine After* Jones, 126 YALE L.J. F. 326, 330 (2017) ("[E]ven if a particular action passes *Jacobsen*'s test (and is thus not a search under *Katz*), it may still be a search under *Jones*.").
25. 831 F.3d 1292 (10th Cir. 2016).

the reasonable expectation of privacy prong and the trespass-to-chattels prong of Fourth Amendment searches will be satisfied.

Part I of this Comment traces the history of the Fourth Amendment's application to computers and details the significant differences between searching a computer and searching a physical space. Part I also summarizes the recent federal circuit split regarding the application of the Fourth Amendment's private search doctrine to computers. The Fifth Circuit[26] and the Seventh Circuit[27] both subscribe to the "physical device" approach: if a private party accessed even just one file on a computer, the entire computer was searched by that private party, and therefore, the police can access the entire computer without conducting a search to which the Fourth Amendment applies. By contrast, the Sixth Circuit[28] and Eleventh Circuit[29] both subscribe to a data or "file" approach: if a private party searched one file on a computer, only that file can be searched by the police. The latter decisions from the Sixth and Eleventh circuits trigger several questions about the file approach.[30] For example, if the private party only viewed one file on the computer, should the police be limited to searching only that single file, or should the police be allowed to search other files contained within the same folder? Is a folder a file? If a private party observed only part of a file on the screen, should the police be allowed to search the remaining contents of that file (e.g., scrolling through a Word document)? Part I of this Comment will also discuss the reintroduction of the trespass-to-chattels definition of a Fourth Amendment search and the implications of that paradigm shift for the private search doctrine.

Part II of this Comment provides a brief summary of the facts, opinions, and holdings of *Ackerman*. Part III first analyzes the Tenth Circuit's reasoning in *Ackerman*, with a particular emphasis on the alternative holding.[31] The last half of Part III endorses the file framework for administering the Fourth Amendment in computer searches. It explains why the file approach is superior to previously-considered approaches and also why the file approach is the most appropriate framework in light of *Ackerman*, *Jones*, and *United States v. Jacobsen*.[32] Furthermore, if courts continue to recognize property rights in data, applying the file approach

26. *Runyan*, 275 F.3d at 464.
27. Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012).
28. *Lichtenberger II*, 786 F.3d 478, 490–91 (6th Cir. 2015).
29. United States v. Sparks, 806 F.3d 1323, 1335 (11th Cir. 2015).
30. *See* Orin Kerr, *11th Circuit Deepens the Circuit Split on Applying the Private Search Doctrine To Computers*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/02/11th-circuit-deepens-the-circuit-split-on-applying-the-private-search-doctrine-to-computers (noting that the deepening circuit split regarding the application of the private search doctrine to computers is ripe for Supreme Court review).
31. *See infra* text accompanying notes 211–14.
32. 466 U.S. 109 (1984).

to Fourth Amendment computer searches emerges as the preeminent logical framework.

I. BACKGROUND

The dawn of the digital age has produced a wide range of new Fourth Amendment complications.[33] Not only have courts been faced with privacy concerns regarding electronic devices, but they also have been forced to consider the ever-increasing storage capacities of computers and smartphones.[34] Section A details the history of Fourth Amendment jurisprudence, the Court's doctrine regarding information previously accessed by private parties, and its application to electronic devices. Section B focuses on the current federal circuit split regarding the contours of the private search doctrine's application to computers. Finally, Section C discusses the trespass-to-chattels doctrine under *Jones* and its impact on the private search doctrine under *Jacobsen*.

A. The Fourth Amendment in the Digital Age

The Fourth Amendment of the U.S. Constitution protects citizens from unreasonable searches and seizures of their "person, houses, papers, and effects."[35] Current Fourth Amendment jurisprudence defines a search in one of two ways. Since the Supreme Court's 1967 decision in *Katz*, a search occurs when a governmental employee or agent of the government violates an individual's reasonable expectation of privacy.[36] In 2012, the Supreme Court supplemented the *Katz* "reasonable expectation of privacy" doctrine by reintroducing the trespass doctrine.[37] Under the *Jones* trespass doctrine, a trespass into an individual's property constitutes a Fourth Amendment search.[38] Thus, even in the absence of a reasonable expectation of privacy, the government may still trigger the Fourth Amendment if it trespasses into a person's property.

One way the Fourth Amendment grants government agents the power to conduct reasonable searches is after receiving a proper warrant.[39] Besides a growing list of exceptions,[40] warrantless searches and

33. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2480 (2014) (analyzing constitutionality of searching cell phone data after arrest); United States v. Jones, 565 U.S. 400, 402 (2012) (analyzing whether attaching a GPS device to defendant's vehicle was a trespass under the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 29 (2001) (analyzing constitutionality of using a thermal imaging device from a public street to scan a private home).

34. *See Riley*, 134 S. Ct. at 2489 (discussing the ever-increasing storage capacities of electronic devices).

35. U.S. CONST. amend. IV.

36. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

37. United States v. Jones, 565 U.S. 400, 412 (2012).

38. *See id.*

39. *See id.* at 406–07.

40. *See* Arizona v. Gant, 556 U.S. 332, 351 (2009) (allowing a search incident to lawful arrest); *see also* Horton v. California, 496 U.S. 128, 130 (1990) (allowing a plain view exception to the Fourth Amendment); Illinois v. Rodriguez, 497 U.S. 177, 181 (1990) (allowing a search "when

seizures are unreasonable on their face.[41] When determining whether to exempt a search from the warrant requirement, courts have generally attempted to conduct a balancing assessment between an individual's privacy and the government's interest in gathering evidence.[42] However, these Fourth Amendment protections only apply to governmental entities or agents.[43] An unreasonable search or seizure conducted by a private individual is exempt from the aforementioned limitations unless the individual who conducted the search was acting under the direction of a government official or agent.[44] In *Jacobsen*, the U.S. Supreme Court articulated the private search reconstruction doctrine (private search doctrine).[45] Under the private search doctrine, when a private party's search violates a person's privacy, a government agent's warrantless search does not violate the Fourth Amendment if it simply replicates the same search already conducted by the private party.[46] The rationale is that a private search extinguishes an individual's reasonable expectation of privacy.[47] Furthermore, the private search doctrine allows a government official to conduct a follow-up search within the scope of the initial search;[48] however, if the government exceeds that scope, then its search will be in violation of the Fourth Amendment.[49]

Jacobsen involved a search of a package by a government agent after Federal Express (FedEx) employees intercepted and searched the same package upon noticing the presence of a suspicious white powder.[50] In addition to replicating the search conducted by the FedEx employees, a Drug Enforcement Agency (DEA) agent also tested the white powder and identified the powder as cocaine.[51] The FedEx employees only searched the package but did not test the white powder.[52] Based on the field test results from the DEA agent and other supporting evidence, the DEA obtained a warrant to search the addressee's home.[53] The DEA

---

voluntary consent has been obtained"); Maryland v. Dyson, 527 U.S. 465, 466–67 (1999) (allowing a motor vehicle exception to the Fourth Amendment).

41. *Katz*, 389 U.S. at 357 ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . .").

42. Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[W]e generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, 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 governmental interests.'") (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

43. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (explaining that Fourth Amendment limitations only apply to governmental searches and seizures).

44. *Id.* (explaining that Fourth Amendment protections do not apply to unreasonable searches by private persons).

45. *Id.* at 117–18.

46. *Id.*

47. *Id.*

48. *Id.* at 115.

49. *See id.* at 117–18.

50. *Id.* at 111.

51. *Id.* at 111–12.

52. *Id.*

53. United States v. Jacobsen, 683 F.2d 296, 298 (8th Cir. 1982), *rev'd*, 466 U.S. 109 (1984).

subsequently found more incriminating evidence and arrested Jacobsen.[54] After denying Jacobsen's motion to suppress the evidence, the U.S. District Court for the District of Minnesota convicted Jacobsen of possession with intent to distribute cocaine and conspiracy to distribute cocaine.[55]

Jacobsen appealed the district court decision, and the U.S. Court of Appeals for the Eighth Circuit held that the DEA agents' field test of the white powder expanded the scope of the private search and thus required a warrant.[56] The Eighth Circuit reversed Jacobsen's convictions, and the Supreme Court granted certiorari.[57] The Court adopted the "virtual certainty" test, which states that to determine whether the government's search exceeded the scope of the initial private search, courts must conduct a balancing test between the amount of information the government stands to gain and the level of certainty regarding what they will find.[58] If the officer is "virtually certain[]" that nothing new will be discovered, then the government's search is within the scope of the initial search.[59] Applying the virtual certainty standard specifically to the DEA agents' field tests, the Court reasoned that the suspicious nature of the white powder made it "virtually certain" that it was some sort of contraband.[60] In short, the government's apparent search was no search at all for Fourth Amendment purposes because it compromised no "legitimate privacy interest."[61]

Since *Jacobsen*, courts have focused on the nature of the area being searched when applying the virtual certainty test.[62] For example, in *United States v. Allen*,[63] the U.S. Court of Appeals for the Sixth Circuit declined to extend the private search doctrine to a search of a motel room.[64] The Sixth Circuit distinguished its holding from *Jacobsen*, citing the material differences between a suspicious package and a motel room.[65] In balancing individual privacy interests with the government's interest in obtaining evidence, the court noted that the package in *Jacobsen* contained only contraband, whereas the motel contained numerous other personal possessions irrelevant to the search.[66]

More recently in *Riley v. California*,[67] the U.S. Supreme Court made an effort to protect data privacy.[68] After police pulled over defend-

54. *Id.*
55. *Id.*
56. *Id.* at 299–300.
57. *Jacobsen*, 466 U.S. at 112–13.
58. *Id.* at 119.
59. *Id.*
60. *Id.* at 124–25.
61. *Id.* at 123.
62. *See* United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997).
63. 106 F.3d 695 (6th Cir. 1997).
64. *Id.* at 699.
65. *Id.*
66. *Id.*
67. 134 S. Ct. 2473 (2014).

ant Riley for a minor traffic infraction, the police searched his phone, revealing gang-related content that tied Riley to a shooting that occurred weeks prior.[69] The government argued that permitting warrantless searches of cell phones incident to arrest could ultimately prevent destruction of evidence and aid law enforcement officers.[70] The Supreme Court rejected this argument, reasoning that cell phones represent an important privacy interest that must be protected because of the significant volumes of personal information contained within them.[71] To protect this privacy interest, the Court held that police officers must obtain a warrant before searching a cell phone.[72] The cellphone in *Riley* is akin to the motel room in the *Allen* case: They both contain numerous pieces of information that may be irrelevant to the search.[73]

To summarize, under the reasonable expectation of privacy definition of a Fourth Amendment search, a search occurs when "[t]he Government's activities . . . violate[] the *privacy* upon which [a person] justifiably relie[s]."[74] However, the Supreme Court has carved out an exception to this definition—the private search doctrine.[75] Under the private search doctrine, once a private party conducts an initial search, the government may repeat that search without triggering a Fourth Amendment "search."[76] With the development of new technology and exponentially increasing storage capacities, applying the private search doctrine to electronic devices has raised unforeseen difficulties and caused splintered decisions.

B. The Private Search Doctrine Circuit Split

Recent circuit court decisions regarding the private search doctrine as applied to computers have led to a circuit split.[77] The split among the circuit courts is rooted in disagreement over the appropriate measuring unit to apply when searching computers:[78] When a private party has

---

68. *Id.* at 2494–95.

69. People v. Riley, No. D059840, 2013 WL 475242, at *1–2 (Cal. Ct. App. Feb. 8, 2013), *rev'd*, 134 S. Ct. 2473 (2014).

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

71. *Id.* at 2494–95.

72. *Id.* at 2495.

73. *Compare* United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997) (remarking that a motel room contains several personal possessions that may be outside the scope of a private search), *with Riley*, 134 S. Ct. at 2494–95 (noting that cell phones may contain several "privacies of life" that may be outside the scope of a private search).

74. Katz v. United States, 389 U.S. 347, 353 (1967) (emphasis added).

75. *See* United States v. Jacobsen, 466 U.S. 109, 117–18 (1984).

76. *Id.*

77. *See supra* note 20 and accompanying text.

78. *Compare* United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001) (holding that the entire physical device was searched), *and* Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012) (holding that the entire physical device was searched), *with Lichtenberger II*, 786 F.3d 478, 491 (6th Cir. 2015) (holding that only the files opened were searched), *and* United States v. Sparks, 806 F.3d 1323, 1335 (11th Cir. 2015) (holding that only the files opened were searched), *and* United States v. Ackerman, 831 F.3d 1292, 1305–06 (10th Cir. 2016).

searched a file on a computer, what exactly has been searched? Has the entire computer been searched? Or has the visible part of the file on the screen only been searched? Or has the entire file itself been searched, regardless if it was displayed in its entirety on the screen? These questions are significant for computer searches, as the answers provide the extent to which government officials are allowed to search a computer absent a warrant after a private citizen has already searched the computer.

In 2001, in *United States v Runyan*,[79] the U.S. Court of Appeals for the Fifth Circuit considered the application of the private search doctrine to digital storage devices containing child pornography.[80] While in the process of moving her things out of the home pending a divorce with her husband, the wife of defendant Robert Runyan discovered CDs and zip disks[81] that contained pornographic images of minors.[82] She turned over the CDs and zip disks to the police, and Runyan was indicted on child pornography charges.[83] Runyan moved to suppress the evidence on the digital storage devices that the law enforcement personnel searched without a warrant.[84] However, the U.S. District Court for the Northern District of Texas denied his motion on the grounds that the police had not exceeded the scope of his wife's initial search.[85]

On appeal to the Fifth Circuit, the court assumed that a computer disk is a closed container in the context of analyzing a warrantless search under the Fourth Amendment.[86] Accordingly, when police officers examine more items of a container than were previously viewed during a private search, the officers do *not* exceed the scope of the initial search.[87] Thus, when the police officers searched the storage devices, they did not exceed the scope of the private search, even though they opened files on the storage devices previously unopened by Runyan's wife.[88] Here, the Fifth Circuit used a physical device measuring unit when reconstructing the private search: because the digital storage device had already been opened and examined to some extent by a private party, the police officers were free to reopen and search all the contents of the digital storage device.[89]

---

79. 275 F.3d 449 (5th Cir. 2001).
80. *See id.* at 456.
81. *Zip Disk*, PC MAG.: ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/55217/zip-disk (last visited Mar. 30, 2017) (providing a definition of zip disk).
82. *Runyan*, 275 F.3d at 452–53.
83. *Id.* at 454–55.
84. *Id.* at 455.
85. *Id.*
86. *See id.* at 464 (treating the computer disk as a closed container).
87. *Id.* at 465.
88. *Id.* at 464–65.
89. *Id.*

Similarly, in 2012, in *Rann v. Atchison*,[90] the U.S. Court of Appeals for the Seventh Circuit held that a more thorough search of a zip drive did not exceed the scope of the previous private search.[91] Defendant Rann was charged with sexual assault and child pornography involving his then-fifteen-year-old daughter.[92] Rann's wife and daughter turned over to police a memory card and a zip drive containing pornographic images of the daughter and another minor.[93] It appeared to the court that Rann's wife had downloaded the images to the zip drive herself.[94] Even though Rann's wife only visibly searched through a few of the files on the zip drive she compiled, the court held that the police's more exhaustive follow-up search of the zip drive did not exceed the scope of the initial search.[95] The court reasoned that because the police were certain that nothing new would be discovered during the follow-up search, the scope of the follow-up search had not been exceeded.[96] Indeed, the court could not "imagine more conclusive evidence that [the defendant's daughter] and her mother knew exactly what the memory card and the zip drive contained."[97]

In 2015, in *United States v. Lichtenberger*,[98] the U.S. Court of Appeals for the Sixth Circuit declined to adopt the physical device (or "closed container") approach of the Fifth and Seventh circuits.[99] Instead, the Sixth Circuit held that police officers exceeded the scope of the prior private search by opening and examining files on the same physical device that the private party searched, but that may not have been viewed by the private party.[100] Defendant Lichtenberger's girlfriend suspected Lichtenberger of possessing child pornography on his computer.[101] Of her own volition, the girlfriend hacked into Lichtenberger's computer using a password recovery program and eventually discovered a folder containing child pornography.[102] The girlfriend contacted the police, and an officer arrived at the house and requested that the girlfriend show him what she had found.[103] The girlfriend "opened several folders and began

90. 689 F.3d 832 (7th Cir. 2012).
91. *Id.* at 838.
92. *Id.* at 834.
93. *Id.*
94. *Id.* at 837.
95. *Id.* at 838.
96. *Id.* (adopting the "substantial certainty" language used in *Runyan*).
97. *Id.*
98. 786 F.3d 478 (6th Cir. 2015).
99. *See* Orin Kerr, *Sixth Circuit Creates Split on Private Search Doctrine for Computers*, WASH. POST (May 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers (arguing that the Sixth Circuit took the correct approach).
100. *Lichtenberger II*, 786 F.3d at 490–91.
101. United States v. Lichtenberger (*Lichtenberger I*), 19 F. Supp. 3d 753, 755 (N.D. Ohio 2014), *aff'd*, 786 F.3d 478 (6th Cir. 2015).
102. *Id.*
103. *Id.*

clicking on random thumbnail images to show him."[104] A warrant was later obtained to search the entire computer, but in later criminal proceedings for possession and distribution of child pornography, Lichtenberger moved to suppress all evidence found on his computer because his then-girlfriend testified that she was not sure the files she showed the police officers were the exact same files she viewed during her private search.[105] Obviously, the same physical device had been searched, but it was not clear that the same files had been searched.[106]

The U.S. District Court for the Northern District of Ohio suppressed the evidence, finding that the private search doctrine did not apply.[107] The Sixth Circuit affirmed the district court's ruling, holding that the police officer exceeded the scope of the prior search because he viewed files that may have differed from those viewed by the private party.[108] Reiterating the concerns from *Riley v. California*,[109] the Sixth Circuit focused on the unique storage capabilities and inevitable privacy interests posed by digital storage devices, concluding that the "virtual certainty" threshold was not met due to the nature of the electronic device.[110] The Sixth Circuit reasoned that the police officer was not virtually certain of what he was to discover on Lichtenberger's computer because the files could not have been viewed without first clicking on them.[111] The Sixth Circuit further remarked that "[o]ther documents, such as bank statements or personal communications, could also have been discovered among the photographs."[112] In short, the Sixth Circuit created a split with the Fifth and Seventh circuits by rejecting the physical device unit of measurement and adopting a file or "data" unit of measurement.[113]

More recently, in *United States v. Sparks*,[114] the U.S. Court of Appeals for the Eleventh Circuit adopted the file or data unit of measurement, which brought the circuit split to 2–2 with regard to how the private search doctrine should apply to computers.[115] In *Sparks*, defendants Johnson and Sparks left their cellphone at a Wal-Mart where a Wal-Mart employee opened it and looked through its contents.[116] The employee found hundreds of disturbing images and videos of child pornography.[117]

104. *Id.*
105. *Lichtenberger II*, 786 F.3d at 481.
106. *See id.*
107. *Lichtenberger I*, 19 F. Supp. 3d at 758–59.
108. *Lichtenberger II*, 786 F.3d at 490–91.
109. 134 S. Ct. 2473, 2495 (2014) (focusing on the significant privacy interests at stake).
110. *Lichtenberger II*, 786 F.3d at 488 (citing *Riley*, 134 S. Ct. at 2489) (discussing unique privacy concerns posed by electronic devices).
111. *Id.* at 481, 489 (noting that the main folder was labeled "private" and sub-folders were "labeled with numbers not words").
112. *Id.* at 489.
113. *See id.* at 489–91.
114. 806 F.3d 1323 (11th Cir. 2015).
115. *See supra* notes 20, 78 and accompanying text.
116. *Sparks*, 806 F.3d at 1329.
117. *Id.* at 1330–31.

The employee told her fiancé, Widner, about the images and videos.[118] Widner searched through the phone, opening a few images and watching one video.[119] Widner then contacted the police, turned over the phone, and showed the officers what he had seen.[120] Subsequently, one of the police officers searched the entire phone—opening all the images to full size and watching a second video that Widner had not viewed.[121]

The Eleventh Circuit held that (1) the police officer who searched the entire phone did not exceed the scope of Widner's private search when he viewed the same images (including thumbnails) and one video that Widner had previously viewed; but (2) the police officer did exceed the scope of Widner's private search when he opened and viewed images and a second video that Widner had not watched.[122] They made this holding despite the fact that the second video was located within the same folder as the first video.[123] Although the "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."[124] Considering the "tremendous storage capacity of cell phones and the broad range of types of information that cell phones generally contain,"[125] the Eleventh Circuit adopted the file approach to the private search doctrine as applied to computers, deepening the circuit split.[126]

Currently, under the reasonable expectation of privacy definition, two circuit courts subscribe to the physical device framework,[127] which holds that a search of a single file on a computer means the entire computer has been searched. Two other federal circuit courts subscribe to a file framework,[128] which essentially holds that the opening of a file constitutes a distinct search. In light of the sharp division among these federal circuit courts, the private search doctrine in computer searches is ripe for Supreme Court review. In fact, in two of the four aforementioned federal circuit cases, petitions for a writ of certiorari were filed.[129] Both were denied.[130]

---

118. *Id.*
119. *Id.*
120. *Id.* at 1331.
121. *Id.* at 1331–32.
122. *Id.* at 1335–37.
123. *Id.* at 1335.
124. *Id.* at 1336.
125. *Id.*
126. *See supra* note 20 and accompanying text.
127. *See* United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001); *see also* Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012).
128. *See Lichtenberger II*, 786 F.3d 478, 491 (6th Cir. 2015); *see also* United States v. Sparks, 806 F.3d 1323 (11th Cir. 2015).
129. Rann v. Atchison, 133 S. Ct. 672 (2012); Sparks v. United States, 136 S. Ct. 2009 (2016).
130. *Atchison*, 133 S. Ct. at 672 (denying petition for certiorari); *Sparks*, 136 S. Ct. at 2009 (denying petition for certiorari).

C. *The Death of the Private Search Doctrine after* Jones

In 2012—forty-five years after *Katz* and twenty-eight years after *Jacobsen*—the U.S. Supreme Court rendered a landmark decision that has raised doubts concerning the viability of the private search doctrine. In *United States v. Jones*, the Court reintroduced the trespass test for what constitutes a Fourth Amendment search.[131] The Court held that the police officers' physical installation of a GPS device on defendant Jones' car was a trespass against Jones' personal effects.[132] This physical intrusion—or trespass—constituted a search per se.[133] The trespass test, revived by *Jones,* requires (1) trespass[134] on (2) a constitutionally protected area[135] (3) "conjoined with . . . an attempt to find something or to obtain information."[136] General Fourth Amendment scholarship teaches that courts utilized the trespass test throughout American history until the 1960s[137] when Justice Harlan's concurring opinion in *Katz v. United States* introduced the two-part expectation-of-privacy inquiry.[138] In the years following the *Katz* decision (in which electronic eavesdropping on a public telephone booth was held to be a search), the vast majority of search and seizure case law has shifted away from that approach founded on property rights and towards an approach based on a person's expectation of privacy.[139] According to Justice Scalia's majority opinion in *Jones*, the *Katz* reasonable-expectation-of-privacy test merely supplemented the pre-*Katz* trespass test.[140]

The reintroduction of the *Jones* trespass test jeopardizes the viability of *Jacobsen.*[141] In *Jacobsen*, the chemical testing of narcotics that resulted in the destruction of a "trace amount" of cocaine was not a search because it failed to reveal more significant information.[142] The reasoning in *Jacobsen* focused only on the reasonable expectation of privacy—the sole test to determine whether a government action was a search when the case was decided.[143] However, by applying the *Jones* trespass test, "the destruction of only a 'trace amount' of private proper-

131. United States v. Jones, 565 U.S. 400, 404–05 (2012); *see also* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 87–91 (2013).

132. *See Jones*, 565 U.S. at 404–05.

133. *Id.*

134. *Id.* at 406.

135. *See id.*

136. *Id.* at 408 n.5.

137. *See id.* at 405 ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.").

138. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining the subjective expectation of privacy and the objective expectation of privacy).

139. *Jones*, 565 U.S. at 406.

140. *See id.* at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

141. *See* United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016) (noting that *Jacobsen* has an "uncertain status" after *Jones*).

142. United States v. Jacobsen, 466 U.S. 109, 123, 125–26 (1984).

143. *Id.* at 122. However, Justice Scalia most likely would have disagreed. *See Jones*, 565 U.S. at 409.

ty" may now be considered a trespass-to-chattels.[144] In fact, even though the defendant's reasonable expectation of privacy was exhausted when the FedEx employees initially opened the package, the government agents' replicated search of the package in *Jacobsen* would be considered a trespass under *Jones*. Under such a theory, the outcome in *Jacobsen* would have been different because destroying the trace amount of powder would have constituted a trespass and, therefore, a search for Fourth Amendment purposes. Ultimately, the property interests protected under *Jones* are more robust than the privacy interests protected under *Jacobsen* because a person's property rights are not eroded when a private party searches (i.e., trespasses) the property. Indeed, a prior private search is completely irrelevant to the *Jones* trespass inquiry.

In the context of computer searches, the private search doctrine's continuing role after *Jones* is questionable. Consider the following fact pattern. Suppose a private party accesses a defendant's computer while the defendant is away at work and uncovers incriminating files. The private party notifies the police, and a police officer arrives at the defendant's residence. The police officer asks the private party to recreate the search that the private party previously conducted so that the officer could view the incriminating files. Because the private party is now an actor under the direction of a police officer, the moment the private party physically touches the computer to begin recreating the prior search is arguably a trespass under *Jones*. Admittedly, under such a broad definition of trespass,[145] it is hard to imagine a scenario where the government's recreation of a prior private search of a computer does not amount to a trespass under *Jones*.

Although *Jones* does not explicitly overrule *Jacobsen*, it does limit the applicability of the private search doctrine to *Katz*-based reasonable-expectation-of-privacy searches.[146] As the *Jones* Court articulated, "Fourth Amendment rights do not rise or fall with the *Katz* formulation."[147] In brief, current Fourth Amendment jurisprudence now has two independent inquiries regarding the definition of a search. Under *Katz*, the sole question is whether the government action invaded an individual's reasonable expectation of privacy.[148] Under *Jones*, the inquiry is whether the government action constitutes a trespass on a constitutionally protected area for the purpose of gathering information.[149] As a result, cases involving government actions that did not constitute a search under *Katz* and *Jacobsen* may have constituted a search under *Jones*. With this

144. *Ackerman*, 831 F.3d at 1307–08.

145. *See Jones*, 565 U.S. at 425 (Alito, J., concurring) ("But under the Court's reasoning, [trivial contact with personal property] may violate the Fourth Amendment.").

146. *Id.* at 407–09 (noting that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test") (majority opinion).

147. *Id.* at 406.

148. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J. concurring).

149. *Jones*, 565 U.S. at 406–07.

background, the U.S. Court of Appeals for the Tenth Circuit decided *United States v. Ackerman.*

II. *UNITED STATES V. ACKERMAN*

A. Facts

AOL, Inc., implements "an automated filter designed to thwart the transmission of child pornography."[150] This image detection filtering process (IDFP) scans images sent, saved, or forwarded from an AOL email account.[151] Additionally, AOL possesses a database of hundreds of thousands of hash values corresponding to pictures meeting the definition of child sexual images.[152] A hash value is "a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value."[153] AOL's IDFP compares the images scanned from emails with the images in the database.[154] If a hash value match is detected, AOL captures the email and prevents the message from sending.[155] AOL also deactivates the user's email account and, pursuant to statutory requirement,[156] forwards the email with its attachments to the National Center for Missing and Exploited Children (NCMEC) through a tool called the CyberTipline.[157]

CyberTipline was launched in 1998 as a way for online users, members of the public, and internet service providers to report suspected child sexual exploitation.[158] Reports can be made online or through the hotline number.[159] Once a report is made with the NCMEC, an analyst opens the file to determine if it meets the definition of child sexual abuse images.[160] NCMEC then utilizes the internet protocol (IP) address and email address of the user to determine the geographic location of the user.[161] NCMEC then alerts law enforcement agents in that geographic area.[162]

---

150. United States v. Ackerman, 831 F.3d 1292, 1294 (2016).
151. United States v. Ackerman, No. 13-10176-01-EFM, 2014 WL 2968164, at *1–2 (D. Kan. July 1, 2014), *rev'd*, 831 F.3d 1292, 1292 (10th Cir. 2016).
152. *Id.*
153. *Ackerman*, 831 F.3d at 1294; *see also* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. 38, 38–40 (2005).
154. *Ackerman*, 2014 WL 2968164 at *2.
155. *Id.*
156. 18 U.S.C. § 2258A(h)(4) (2012); 42 U.S.C. § 5773(b)(P)–(Q) (2012).
157. *Ackerman*, 831 F.3d at 1294.
158. *CyberTipline*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., http://www.missingkids.org/cybertipline (last visited Mar. 30, 2017).
159. *Id.*
160. *See Ackerman*, 831 F.3d at 1294.
161. *See id.*
162. *See id.*

On April 22, 2013, AOL's IDFP detected a hash value match on one of defendant Ackerman's four outgoing email attachments.[163] The aforementioned process was triggered.[164] AOL forwarded a report to NCMEC with the four attached images.[165] An NCMEC analyst opened the email along with all four of the attachments.[166] No warrant was obtained by NCMEC.[167] NCMEC confirmed that all four images met the definition of child pornography and determined that the defendant's location was Kansas.[168] NCMEC then alerted law enforcement agents in the area, and a special agent obtained a warrant to search Ackerman's residence while Ackerman was at work, finding "multiple digital items that revealed the presence of child pornography."[169] A federal grand jury then indicted Mr. Ackerman on charges of possession and distribution of child pornography.[170]

B. Procedural History

The U.S. District Court for the District of Kansas rejected Ackerman's argument that the email and its attachments were "obtained through an illegal search and seizure"[171] and, therefore, denied Ackerman's motion to suppress the evidence.[172] The district court specifically rejected Ackerman's arguments to employ a three-part test from the First Circuit[173] and instead relied on the test the Tenth Circuit articulated in *United States v. Souza*[174]: "A search by a private person becomes a government search if the government coerces, dominates, or directs the actions of a private person conducting the search."[175] "To determine whether a search by a private person becomes a government search, there is a two-part inquiry: '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.'"[176]

Because a law enforcement agent was not present when NCMEC conducted its search, the district court found that a law enforcement

163. United States v. Ackerman, No. 13–10176–01–EFM, 2014 WL 2968164, at *3 (D. Kan. July 1, 2014), *rev'd*, 831 F.3d 1292, 1292 (10th Cir. 2016).
164. *Ackerman*, 831 F.3d at 1294.
165. *Id.*
166. *Id.*
167. *Id.* at 1294–95.
168. *Id.* at 1294.
169. *Ackerman*, 2014 WL 2968164, at *4 (D. Kan. July 1, 2014), *rev'd*, 831 F.3d 1292, 1292 (10th Cir. 2016).
170. *Id.*
171. *Id.*
172. *Id.* at *10.
173. *Id.* at *6–7 (citing United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass. 2013)).
174. United States v. Souza, 223 F.3d 1197 (10th Cir. 2000).
175. *Ackerman*, 2014 WL 2968164 at *5, *7 (citing *id.* at 1201).
176. *Id.* at *5 (quoting *Souza*, 223 F.3d at 1201).

agent did not direct NCMEC.[177] Furthermore, the district court held that NCMEC is a private, non-profit corporation.[178] Alternatively, the district court held that even if NCMEC was considered a government actor, NCMEC did not exceed the scope of AOL's initial search "in such a way that would be constitutionally significant."[179]

Two questions were on appeal to the Tenth Circuit.[180] First, "[D]oes NCMEC qualify as a governmental entity or agent?"[181] Second, if NCMEC does qualify as a governmental entity or agent, "did NCMEC simply repeat or did it exceed the scope of AOL's investigation?"[182]

C. Tenth Circuit Opinion

The U.S. Court of Appeals for the Tenth Circuit disagreed with the district court on both counts.[183] In the first section of the opinion, the Tenth Circuit concluded that NCMEC qualifies as the government for Fourth Amendment purposes.[184] Judge Gorsuch, writing for the court, relied on NCMEC's two authorizing statutes[185] and recent Supreme Court decisions[186] to support this argument.

Even if the Tenth Circuit was wrong in determining that NCMEC is a governmental entity, the court held that NCMEC acted as an agent for the government in this particular case.[187] Judge Gorsuch returned to the Tenth Circuit's two-part inquiry under *Souza*[188] but concluded that regardless of which circuit court test is applied, "it's hard to see how we could avoid deeming NCMEC the government's agent in this case."[189]

In the third part of the opinion, the Tenth Circuit held that if NCMEC is considered a government entity or agent, its actions still implicated the Fourth Amendment, specifically because the actions did not fall within the scope of the private search doctrine.[190] Judge Gorsuch initially pointed out that "[n]o one in this appeal disputes that email is a 'paper' or 'effect' for Fourth Amendment purposes, a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more."[191] However, because the district court assumed that Mr. Ackerman had a

177. *Id.* at *7, *10.
178. *Id.* at *8.
179. *Id.* at *8, *10.
180. United States v. Ackerman, 831 F.3d 1292, 1294–95 (2016).
181. *Id.* at 1295.
182. *Id.*
183. *Id.*
184. *Id.* at 1299.
185. *Id.* at 1296–97.
186. *Id.* at 1297–98 (drawing comparisons between NCMEC and Amtrak).
187. *Id.* at 1300–04.
188. United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000).
189. *Ackerman*, 831 F.3d at 1301–02.
190. *Id.* at 1304–08.
191. *Id.* at 1304.

reasonable expectation of privacy and decided to not analyze the Supreme Court's so-called "third-party doctrine,"[192] the Tenth Circuit declined to reach the broad issue of whether emails are protected under the Fourth Amendment.[193]

Nevertheless, the government argued on appeal that the private search doctrine compelled a ruling in its favor.[194] The Tenth Circuit rejected this argument, noting that "AOL never opened the email itself."[195] AOL only scanned the email and images, found a positive hash-value comparison on one of the attachments with its internal database, and forwarded the email and attachments to NCMEC.[196] Applying *Jacobsen*'s private search doctrine, the Tenth Circuit acknowledged that there was no virtual certainty that the email itself and the other three attachments contained child pornography.[197] "Indeed, when NCMEC opened Mr. Ackerman's email it could have learned any number of private and protected facts . . . ."[198] Because NCMEC's search "could have revealed something previously unknown about noncontraband items," a Fourth Amendment search exceeding the scope of the initial search took place.[199]

In Section B of the third part of the opinion, the Tenth Circuit reached the same conclusion regarding the private search doctrine, but under a different line of reasoning: the *United States v. Jones* trespass test.[200] Section B of the third part of this opinion, which was joined only by Judge Phillips and not Judge Hartz,[201] concluded that when NCMEC opened Ackerman's email message it constituted a physical intrusion or trespass into Ackerman's papers or effects under the *Jones* trespass test.[202] Not only did Judge Gorsuch call into question the continuing viability of *United States v. Jacobsen*,[203] but he also noted that "many courts have already applied the common law's ancient trespass to chattels doctrine to electronic . . . communications."[204] Simply stated, regardless of whether the court applies the *Jacobsen* and *Katz* reasonable-expectation-of-privacy standard or the *Jones* trespass-to-chattels test,

192. *Id.* at 1304–05.
193. *Id.*
194. *Id.* at 1305.
195. *Id.* at 1305–06.
196. *Id.* at 1306.
197. *Id.* at 1305–06.
198. *Id.* at 1306.
199. *Id.*
200. *Ackerman*, 831 F.3d at 1307–08.
201. *Id.* at 1294.
202. *Id.* at 1307–08.
203. *Id.* at 1307.
204. *Id.* at 1308 (citing eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063, 1069–70 (N.D. Cal. 2000); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019, 1027 (S.D. Ohio 1997); Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1565–67 (1996)).

the result is the same: "NCMEC conducted a 'search' when it opened and examined Mr. Ackerman's email."[205]

III. ANALYSIS

A. Ackerman's *Alternative Holding is Binding*

Briefly, Section B of the third part of the opinion is important not only for its "puzzling" and "far-reaching implications"[206] with regard to the *Jones* trespass test and the viability of *Jacobsen* and *Katz*,[207] but also because this section serves as an "alternative holding."[208] Alternative holdings are binding on the Tenth Circuit,[209] which means that the application of the *Jones* trespass test is no longer limited to what is generally considered physical and tangible property.[210]

B. *The* Jones *Trespass Test Applies to "Virtual"*[211] *Property*

United States v. Jones produced significant uncertainty among legal scholars regarding exactly what kind of test it creates.[212] The first Supreme Court case applying the *Jones* trespass test after *Jones* itself was *Florida v. Jardines*.[213] With Justice Scalia writing for the majority, the Court found that when the police officers were gathering information in the "curtilage of the house," they physically entered and intruded into a constitutionally protected area.[214] Some scholars have suggested that after *Jardines* the *Jones* trespass test only applies to the physical intru-

---

205. *Id.*

206. *See* Orin Kerr, *Tenth Circuit: Accessing Email is a 'Search' Under the* Jones *Trespass Test*, WASH. POST (Aug. 9, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/08/09/tenth-circuit-accessing-email-is-a-search-under-the-jones-trespass-test.

207. *See* discussion *supra* Section I.C and discussion *infra* Section III.B.

208. *See* Chinua Asuzu, JUDICIAL WRITING: A BENCHMARK FOR THE BENCH 134 (2016) ("Alternative holdings are separate and independent grounds for a decision.").

209. *See* Surefoot LC v. Sure Foot Corp., 531 F.3d 1236, 1243 (10th Cir. 2008) ("Alternative rationales such as this, providing as they do further grounds for the Court's disposition, ordinarily cannot be written off as *dicta*.").

210. United States v. Jones, 565 U.S. 400, 405 (2012) ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a *physical intrusion* would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." (citing Entick v. Carrington (1765) 95 Eng. Rep. 807 (K.B.)) (emphasis added). Even though the property is not limited to only physical and tangible assets, the trespass itself must be physical per *Jones*.

211. From a physics perspective, there is no such thing as "virtual" objects. All "virtual" electronic data is tangible because it exists in computer memory in the form of magnetic particles (i.e., electrons). *See, e.g.*, C. Claiborne Ray, *The Weight of Memory*, N.Y. TIMES (Oct. 24, 2011), http://www.nytimes.com/2011/10/25/science/25qna.html.

212. *See* Kerr, *supra* note 131, at 90–93; *see also* Marc J. Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 26–32 (2013); *see also* Susan Freiwald, The Four Factor Test (2013) (unpublished manuscript) (on file with the University of San Francisco); *see also* US v. Jones, *From Jones to Drones: How to Define Fourth Amendment Doctrine for Searches in Public*, YOUTUBE (June 24, 2012), https://www.youtube.com/watch?v=_pGCWZGdq08.

213. 133 S. Ct. 1409 (2013).

214. *Id.* at 1414.

sion of property, not virtual property.[215] However, if courts define electronic communications, such as emails and text messages, as an individual's papers or effects under the Fourth Amendment,[216] then a police officer who intrudes into those spaces without a warrant is intruding into a constitutionally protected area. Simply because emails, text messages, and other electronic forms of communications are not physically tangible in the sense that an individual cannot physically touch or hold them—absent printing the electronic communications on physical paper—does not mean that such electronic communications lack the necessary "physical" aspect of the *Jones* trespass test. For a computer, most electronic data is physically stored on a hard disk drive.[217] A traditional hard disk drive is a physical and tangible object comprised of a spinning disk or disks with magnetic coatings and heads that can read or write magnetic information.[218] These read-write heads[219] record binary numbers as a series of tiny physical areas on the disc that are magnetized either north or south (i.e., 0's and 1's).[220] "As the disk spins, a laser is either reflected or not reflected by a series of tiny mirrored sections on the disk."[221] Alternatively, a more modern solid-state drive (SSD) does not rely on moving parts or spinning disks, but instead relies on flash memory.[222] A charged electron corresponds to a "0," whereas an uncharged electron corresponds to a "1" in bit code.[223] Electrons are physical atoms that have mass.[224] Thus, when the government accesses electronic data, it physically intrudes on papers or effects under the Fourth Amendment because the government is obtaining information by physically extracting

215. *See* Orin Kerr, *What is the State of the* Jones *Trespass Test After* Florida v. Jardines*?*, VOLOKH CONSPIRACY (March 27, 2013, 2:56 AM), http://volokh.com/2013/03/27/what-is-the-state-of-the-jones-trespass-test-after-florida-v-jardines/ ("[P]erhaps the *Jones* test is not about the technicalities of trespass doctrine but rather about physical intrusion into property.").

216. *See* United States v. Ackerman, 831 F.3d 1292, 1307–08 (2016).

217. ANDREW S. TANENBAUM & HERBERT BOS, MODERN OPERATING SYSTEMS 281, 300 (4th ed. 2015) ("File systems are stored on disks.").

218. *Hard Disk*, PC MAG.: ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/44079/hard-disk (last visited Mar. 30, 2017).

219. *Read/Write Head*, PC MAG.: ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/50247/read-write-head (last visited Mar. 30, 2017).

220. *See id.*; *see also* Timothy Smithee, *How is Data Stored in a Computer?*, TECHWALLA, https://www.techwalla.com/articles/how-is-data-stored-in-a-computer (last visited Mar. 30, 2017); *see also* JAMES R. PARKER, PYTHON: AN INTRODUCTION TO PROGRAMMING Ch. 5 (Mercury Learning & Information, 2016) ("Magnets have two orientations; they have a North Pole and a South Pole. Current flowing one way will create a magnet in the disk that has a North Pole appearing before the South Pole, or an N-S mark. Current flowing the other direction through the head will create a magnet on the disk that has the South Pole appearing before the North Pole, or an S-N mark. One orientation, say N-S, will represent a binary number '1,' and the other (S-N) will represent a '0.' In this way, binary numbers can be written to the surface of the moving disk.").

221. *See id.*

222. Joel Hruska, *How Do SSDs Work?*, EXTREMETECH (May 3, 2017, 3:23 AM), https://www.extremetech.com/extreme/210492-extremetech-explains-how-do-ssds-work.

223. *Id.*

224. 1 electron = 9 x 10^{-31} kg. *Fundamental Physical Constants*, NIST REFERENCE ON CONSTANTS, UNITS, AND UNCERTAINTY, http://physics.nist.gov/cgi-bin/cuu/Value?me (last visited Mar. 30, 2017).

the binary data that is physically encoded onto a physical hard disk drive with magnetic coatings or electrons.

The U.S. Court of Appeals for the Seventh Circuit recently elaborated upon the *Jones* trespass test by establishing a two-part inquiry[225]: Triggering a *Jones* trespass requires (1) confirming "possession of the property in question" and (2) establishing "the ability to exclude others from entrance onto or interference with that property."[226] In the context of electronic data, the first step of the Seventh Circuit's inquiry poses an initial problem: if an individual's data is accessed on a government hard disk drive (e.g., a private party sends the data to the government on its own volition), who has possession of the property? By adhering to the aforementioned principles regarding the physical nature of electronic data, this problem is solved by recognizing property rights within data itself. Not only does this solution comport with the first step of the Seventh Circuit's inquiry, but it also agrees with the physical characteristics of the *Jones* test. An individual's copied data on a government-owned hard disk drive is still property of the individual under the data-rights theory. Furthermore, even if a court disregarded the physical properties of electronic data, such an interpretation does not vex the *Jones* test because accessing the data (i.e., the "property") still requires entrance into a physical space, such as a physical hard disk drive, random access memory (RAM), solid state drive, or memory chip commonly found in USB keys, SD cards, MP3 players, and cell phones.[227] Accessing data will always require physical intrusion into a physical space, regardless of how physically small that space may be.[228]

The second step in the Seventh Circuit's inquiry is easily satisfied in the context of electronic data. For example, a closed laptop computer would satisfy the second step because it is closed for the purpose of excluding others from opening the laptop and accessing the data therein. More robust examples of excluding others "from entrance onto or interference with" data include standard login passwords, two-factor authentication protocols,[229] fingerprint recognition, and verification codes.[230]

---

225. United States v. Sweeney, 821 F.3d 893, 900 (7th Cir. 2016).

226. *Id.*

227. *See supra* text accompanying notes 217–30.

228. *See Magnetic Storage*, PC MAG.: ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/46497/magnetic-storage (last visited Mar. 13, 2017) ("In the digital world, information is recorded by writing tiny spots (bits) of negative or positive polarity on tapes and disks.").

229. *See Two-Factor Authentication*, PC MAG.: ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/53279/two-factor-authentication (last visited Mar. 30, 2017).

230. *See* Eric Griffith, *Two-Factor Authentication: Who Has It and How to Set It Up*, PC MAG. (Mar. 10, 2017), http://www.pcmag.com/article2/0,2817,2456400,00.asp.

In short, the *Jones* trespass-to-chattels standard[231] is not hindered when applied to virtual property because (1) electronic data is stored in physical spaces; (2) electronic data is only accessed by intruding into the physical area where the electronic data is stored; and (3) electronic data commands a physical property right within itself.

C. Applying Jones *to* Ackerman

Returning to *Ackerman*, Judge Gorsuch failed to explain why the elements of the *Jones* trespass-to-chattels tort were satisfied in this particular case.[232] Rather, he simply relied on an analogy between the ordinary postal system and email, assuming that the analogy speaks for itself.[233] Although email and regular mail are analogous,[234] the details of why the elements of trespass are satisfied in this case should be clarified. First, the test articulated by the Tenth Circuit states "that government conduct can constitute a Fourth Amendment search . . . when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ('persons, houses, papers, and effects') for the purpose of obtaining information."[235] Applying this standard to the facts and drawing from the aforementioned reasoning in Section B, Ackerman possessed a physical property right within the data of the email itself. Thus, although AOL copied the email with all of its data and forwarded it to NCMEC, Ackerman's property right in the data still existed. Furthermore, even though NCMEC supposedly stored Ackerman's email on its own physical storage device(s), Ackerman still retained a physical property right in the data itself. Next, NCMEC's act of opening Ackerman's email and thereby exposing his electronic data constituted a physical intrusion into a constitutionally protected space or thing, namely papers and effects. As previously mentioned, the act of opening electronic data requires a physical intrusion into a physical space on a physical memory device.[236] Thus, (1) possession of the property is established by finding a property right within the data itself, and (2) physical intrusion into that property is established by the act of impermissibly opening the email file that resides on a physical memory device containing the data, regardless if the suspect has physical possession of that particular memory device.

---

231. United States v. Jones, 556 U.S. 400, 404–07 (2012).

232. *See* United States v. Ackerman, 831 F.3d 1292, 1307–08 (10th Cir. 2016).

233. *Id.* at 1308 ("[A] more obvious analogy from principle to new technology is hard to imagine . . . .").

234. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1023 (2010).

235. *Ackerman*, 831 F.3d at 1307.

236. *See supra* text accompanying notes 217–30.

D. The File Approach and the Reasonable Expectation of Privacy

The majority of data located on a computer or other electronic device resides in a structure called a "filesystem."[237] A filesystem simply describes the way in which files are named and where they are placed logically for storage and retrieval among the hard disk drive, RAM, and external memory devices.[238] A file is simply a collection of data or information and serves as a computer's primary storage unit.[239] With this technical backdrop in mind, a simple framework for determining a person's reasonable expectation of privacy can be derived: When a file is opened on a computer, no reasonable expectation of privacy exists with regard to that opened file; when a file is closed on a computer, a reasonable expectation of privacy attaches with regard to that closed file. The file approach adequately comports with the reasonable expectation of privacy doctrine.

In the context of physical and tangible searches, a house is searched when a government agent enters it,[240] and a package is searched when a government agent opens it.[241] Individuals should have a reasonable expectation of privacy in their personal files just as individuals have a reasonable expectation of privacy in their home and packages. A person's data in a file is his or her private property and should be treated no differently than other privately sealed containers.[242] Since a person has a reasonable expectation of privacy in the contents of the container,[243] opening the container and seeing the contents constitutes a distinct Fourth Amendment search and violates the reasonable expectation of privacy. Applying these same foundational principles to computers, a closed file is analogous to a closed container, whereas an opened file is analogous to an opened container. Similarly, the act of double-clicking to open a previously unopened file is analogous to the act of physically opening a closed container. As demonstrated, the file approach accurately corresponds to the physical world notions of Fourth Amendment searches. "A computer is akin to a virtual warehouse of private information,"[244] and accordingly, a single file stored in a computer's hard drive is akin to a single container or box stored inside the warehouse. There is no reasonable expectation of privacy in an already-opened con-

237. TANENBAUM, *supra* note 217, at 264.
238. *Id.* at 42, 264.
239. *Id.* at 264.
240. *See* Wilson v. Layne, 526 U.S. 603, 610 (1999).
241. *See* United States v. Ross, 456 U.S. 798, 822–23 (1982).
242. *See* United States v. Blas, No. 90-CR-162, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) ("[A]n individual has the same expectation of privacy in a pager, computer or other electronic data storage and retrieval device as in a closed container . . . .").
243. *Id.*
244. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551–52 (2005).

tainer just as there should be no reasonable expectation of privacy in an already-opened file.

Alternative methodologies to the file approach yield imbalanced results. For example, consider the physical device approach, which states that once a single file has been searched on an electronic device, the entire electronic device no longer commands a reasonable expectation of privacy.[245] In the age of cloud technology and remote servers, a group of physical storage devices in a data warehouse can house files belonging to hundreds of millions of individuals.[246] Thus, absurd outcomes would be inevitable if looking at one file on a remote server meant that the entire server had been searched, and therefore, the government could analyze all the files stored on that server, allowing unrestricted access to potentially millions of documents belonging to other people. Such a problem is also compounded by the current debate as to whether cloud-based data even deserves Fourth Amendment protections initially.[247] As suggested in *Ackerman*[248] and previously proposed in Section C,[249] the Fourth Amendment should track the individual's data, not the physical device where the data is stored.

Although not as obvious as the physical device approach, concerns also exist with the human observation approach.[250] The human observation approach advocates that the scope of a computer search should be limited to "whatever information appears on the output device."[251] "Under this approach, scrolling down a word processing file to see parts of the file that were previously hidden is a distinct search of the rest of the file."[252] However, this would imply that the zone of a computer search could be oddly defined, for example, by the "zoom" tool for a document. Zooming out of the document would allow more pages of the document to be displayed on the screen, whereas zooming in to the document would allow less pages to be displayed. Similarly, the human observation standard yields odd results regarding pixilated images. A person could easily enhance a blurry image displayed on a screen by adjusting the image size (e.g., increasing screen resolution or pixel volume).[253] In both examples, the human observation standard is uncertain. In the document

245. *See supra* text accompanying notes 25–26, 127.

246. *See, e.g.*, Drew & Arash, *Celebrating Half a Billion Users*, DROPBOX BLOG (Mar. 7, 2016), https://blogs.dropbox.com/dropbox/2016/03/500-million.

247. *See* Aaron J. Gold, *Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software*, 56 WM. & MARY L. REV. 2321, 2325 (2015); *see also* Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J.F. 73, 73–74 (2014).

248. *See supra* text accompanying notes 183–205.

249. *See supra* text accompanying notes 232–36.

250. *See* Kerr, *supra* note 244, at 556.

251. *Id.*

252. *Id.* at 556–57.

253. A similar issue arises when considering thumbnail images because thumbnails are usually smaller and less clear than full images. *See, e.g.*, *Lichtenberger II*, 786 F.3d 478, 480–81 (6th Cir. 2015) (addressing thumbnails, which are smaller versions of the file's images).

example, the government technically "observed" the document, but the extent of the observation was tied to the "zoom" tool. In the picture example, the government technically "observed" the picture, but the extent of the observation was tied to the resolution of the image. Such ambiguities will likely spawn unnecessary obstacles during litigation.

The best definition for the zone of a computer search is the file. As previously stated, individuals should have a reasonable expectation of privacy in their personal files. Using a file as the zone of a computer search eliminates several of the complications that accompany both the physical device approach and the human observation approach. Most importantly, the file approach comports with the reasonable expectation of privacy doctrine and is easy to apply: When a file is opened on a computer, no reasonable expectation of privacy exists with regard to that opened file; when a file is closed on a computer, a reasonable expectation of privacy attaches with regard to that closed file.

E. The File Approach and Trespass

When a file is opened on a computer, a series of complicated physical steps occur.[254] First, the filesystem code is invoked to read raw bytes from the disk and interprets those byte patterns as a tree of files and directories.[255] The filesystem then translates a user instruction such as "Open file X" into individual machine-readable input/output instructions.[256] The input/output instructions use the built-in capabilities of the processor chip[257] and the motherboard controller[258] to send and receive electrical signals on a wire going to the physical drive. On the other end of this wire, the disk's firmware[259] interprets the electrical signals and then accesses the physical data through methods such as spinning the platters[260] and moving the magnetic heads or reading a flash ROM cell.[261] The method necessary to access the desired data depends on the type of storage device housing the data.[262] Notwithstanding the type of storage device housing the data or where the data is located on that storage device, in order to access any type of data, a device must always execute physical actions of sending and receiving electrical signals.

---

254. TANENBAUM, *supra* note 217, at 288.

255. *See id.*

256. *See id.* ("machine-readable" meaning bit code (i.e., 0's and 1's)).

257. *Id.* at 21 (describing the central processing unit as the "brain" of the computer).

258. *Id.* at 34 (motherboard contains low-level input/output software, "including procedures to read the keyboard, write to the screen, and do disk I/O, among other things").

259. *Id.* at 893 (software that is loaded on PCs by the manufacturer and "persists in memory").

260. *Id.* at 27 ("A disk consists of one or more metal platters that rotate at 5400, 7200, 10,800 RPM or more.").

261. *Flash Memory*, PC MAG.: ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/43272/flash-memory (last visited Mar. 30, 2017) (defining "flash memory" and noting their replacement of spinning platters).

262. *See* TANENBAUM, *supra* note 217, at 1025.

By using this technical foundation and recognizing a unique property right within data itself, a trespass of an electronic device should be defined by opening a file rather than broadly defined as any physical manipulation of the device (e.g., merely touching the device would constitute a trespass under *Jones*). Adopting this narrower definition of trespass produces two clear benefits. First, the private search doctrine as applied to computers can be preserved. A police officer who recreates the exact prior private search is no longer hindered by the "trivial"[263] nuances of physically touching a computer that would otherwise constitute a trespass under *Jones*.[264] Specifically, a police officer would be allowed to touch, scroll, and click on a computer during the recreation of the prior private search without triggering a trespass, as long as new files that were previously closed during the prior search are not opened.

Secondly, by focusing on the file as opposed to the physical device, a trespass can now occur even if the suspect's data is not accessed on the suspect's computer. Consider *Ackerman*: If a trespass was defined as a physical intrusion on the physical device, then the government's access of Ackerman's email would not technically be a trespass because AOL captured the email and forwarded that data to NCMEC.[265] NCMEC did not obtain a warrant to search through Ackerman's data,[266] but nonetheless, under a definition of trespass that only focuses on physical intrusions of the physical device, NCMEC would not have triggered a unique Fourth Amendment search under the trespass-to-chattels definition because it did not access the data on Ackerman's physical device. Conversely, this problem is solved by couching the definition of trespass in the unit of a computer file. Regardless of where the data was accessed, a trespass occurred the moment NCMEC opened Ackerman's files without a warrant.[267] The "chattel" that is trespassed is the data, not the electronic device where the data is stored.

A main critique of the file approach is that "much information stored on a computer does not appear in a file."[268] This is a baseless concern because the information on a computer that is technically not stored in a file *per se* is stored physically in magnetic strings of 0's and 1's on a disk.[269] In other words, the information not stored in a file cannot be read by humans without first converting that information into a file of some sort. Moreover, by adopting a broad definition of file,[270] a coherent ar-

263. *See* United States v. Jones, 565 U.S. 400, 425 (2012) (Alito, J., concurring) ("But under the Court's reasoning, [trivial contact with personal property] may violate the Fourth Amendment.").
264. *Id.* at 424–25 (Alito, J., concurring).
265. *See supra* text accompanying notes 150–70.
266. *See supra* text accompanying notes 150–70.
267. *See supra* text accompanying notes 150–70.
268. Kerr, *supra* note 244, at 557.
269. *See supra* text accompanying notes 217–30.
270. *See supra* text accompanying note 246.

gument could be made that the collection of physical information stored on a disk is still considered a file.

The Fourth Amendment trespass-to-chattels search doctrine as applied to electronic devices should be defined by files and not physical devices. A file is directly analogous to real property because the file structure itself represents the "fence" of the property, and the data contained within the file represents the land and other possessions contained within the fence. The conceptual framework is simple: opening a file is akin to crossing the fence of real property.[271]

F. The File Approach in Practice

Another reason for adopting the file approach is that the actions of opening and closing a file trigger clear physical movements within the hard drive of a computer that are corroborated by timestamp metadata.[272] When an analyst takes a mouse, clicks, and scrolls down the file to see parts of the file not previously exposed, no other files or information contained outside of the already-opened file are copied to the RAM,[273] and the standard metadata in the file is not altered.[274] Thus, maintaining the integrity of the human observation standard becomes problematic because few alternative sources of evidence exist to prove whether an analyst "scrolled through" or "zoomed in on" a document or image, especially without some type of "saved state" operation.[275] Additionally, adhering to a physical-device-based definition of trespass is also problematic because few alternative sources of evidence exist to prove whether or not an analyst touched a computer, opened a laptop, and scrolled through a document. Fortunately, the file approach is supplemented by several accountability mechanisms built-in to most electronic devices.[276] For example, a timestamp is recorded when a file is opened or

271. *See, e.g.*, *Lichtenberger II*, 786 F.3d 478, 480–81 (6th Cir. 2015) (illustrating that the act of clicking on a thumbnail to open the file constitutes a distinct search); *see also* United States v. Sparks, 806 F.3d 1323, 1330–31 (11th Cir. 2015) (concluding that an officer opening a previously unopened file is a distinct search).

272. TANENBAUM , *supra* note 217, at 956 ("The standard information field contains the file owner, security information, the timestamps needed . . . .").

273. *Id.* at 433 ("To scroll a window, the CPU (or controller) must move all the lines of text upward by copying their bits from one part of the video RAM to another.").

274. *See id.* at 271 (explaining that standard metadata attributes do not include state information).

275. *Id.* at 829 (describing the Android OS that provides a "saved state" operation and explaining that "[t]he saved state for an activity is generally small, containing for example where you are scrolled in an email message, but not the message itself, which will be stored elsewhere by the application in its persistent storage").

276. *See, e.g.*, Whitson Gordon, *How to Find Out if Someone's Secretly Been Using Your Computer*, LIFEHACKER (Jan. 5, 2012, 4:30 PM), http://lifehacker.com/5873538/how-to-find-out-if-someones-secretly-been-using-your-computer; *see also* Matthew Panzarino, *Paranoid? Here's How to Tell if Anyone Has Opened Your MacBook While You're Away*, NEXT WEB (Jan. 3, 2012), https://thenextweb.com/apple/2012/01/04/paranoid-heres-how-to-tell-if-anyone-has-opened-your-macbook-while-youre-away.

closed.[277] When a file is saved and closed, it is stored to a specific partition on the hard drive disk, which alters the metadata in the file.[278] In short, an analyst who double clicks to open a file is doing something fundamentally different than an analyst who simply scrolls through an already-opened file. The former's actions are far more ascertainable and concrete, whereas the latter's actions will result in frivolous uncertainties that lack other means of authentication. Using the file as the unit of measurement to define a computer search is the superior approach.

Most importantly, lawyers will be able to more adequately advocate these issues on behalf of their clients. Because courts will be analyzing the open/close timestamps of files on a storage device,[279] discovery and introduction of evidence is straightforward. Although law enforcement officers may still be able to testify about what they "opened" or what they "saw" during the reconstructive search, more weight should be given to the more objective evidence located on the storage devices. Additionally, the file approach removes many of the abstract technicalities of computer functionality because lawyers, judges, and analysts will only be concerned with whether a particular file was "open" or "closed." Under a human observation approach of the reasonable expectation of privacy definition,[280] many cases would require the consultation of technical experts to attempt to reconstruct the exact portions of the file that were exposed on the screen, even if those portions of the files were captured for only a nanosecond and no metadata record of them was retained. Fortunately, equipped with the more well-defined file standard, judges will be able to more adequately render appropriate decisions under both the reasonable expectation of privacy doctrine[281] and the trespass-to-chattels doctrine.[282] A possible bright-line rule emerges from the file approach that comports with both definitions of a Fourth Amendment search: As established by a timestamp and metadata analysis, accessing a file that is already-opened is not a Fourth Amendment search. However, opening a previously-closed file triggers a unique Fourth Amendment search in the absence of a warrant.

CONCLUSION

As technology continues to rapidly evolve, more complications will inevitably arise regarding the Fourth Amendment's application to computers and other electronic devices. Within the last two decades, two

277. TANENBAUM, *supra* note 217, at 271 ("The various times keep track of when the file was created, most recently ac[]cessed, and most recently modified.").

278. *Id.* at 272–73 ("A disk is written in blocks, and closing a file forces writing of the file's last block . . . .").

279. *See infra* text accompanying note 286.

280. *See supra* text accompanying notes 250–53.

281. *See supra* text accompanying notes 237–53.

282. *See supra* text accompanying notes 254–73.

circuit courts have adopted a concerning physical device approach,[283] whereas three other circuit courts have adopted a more stringent file approach.[284] The deepening split among the federal circuit courts with regard to the private search doctrine's application to computers makes this issue ripe for Supreme Court review in the imminent future. Moreover, the re-emergence of the *Jones*[285] trespass test further confounds existing Fourth Amendment doctrine. Thus, once the opportunity arises, it is imperative for the Supreme Court to articulate a viable and consistent framework that is flexible enough to adapt to the ever-changing digital landscape.

The file approach is the most viable, consistent, and flexible framework with regard to Fourth Amendment computer searches. All programs and human-readable data on a computer are contained in a file, from Microsoft Word documents (.DOC files) to JPEG images (.JPG files) to executable applications (.EXE files).[286] In fact, the architectural underpinnings of computer storage are built upon the concept of a file system.[287] Unless the underlying hardware of electronic devices and computers abruptly departs from the foundational file and file system data structures, the file approach to Fourth Amendment computer searches will remain a clear and steadfast framework for generations to come.

Roderick O'Dorisio[*]

283. *See* United States v. Runyan, 275 F.3d 449, 463–464 (5th Cir. 2001); *see also* Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012).

284. *See Lichtenberger II*, 786 F.3d 478, 491 (6th Cir. 2015); *see also* United States v. Sparks, 806 F.3d 1323, 1335 (11th Cir. 2015); *see also* United States v. Ackerman, 831 F.3d 1292, 1304–08 (10th Cir. 2016).

285. United States v. Jones, 565 U.S. 400, 406–07 (2012).

286. TANENBAUM, *supra* note 217, at 4 (noting that all operating systems contain files in order to avoid "having to deal with the messy details of how the hardware actually works").

287. *Id.* at 41 ("Another key concept supported by virtually all operating systems is the file system.").

* Roderick O'Dorisio is a Staff Editor on the *Denver Law Review* and a 2018 J.D. Candidate at the University of Denver Sturm College of Law. He holds a B.S. in Computer Science from the University of Denver and is a registered patent agent. He would like to thank Professor Ian Farrell for providing an abundance of helpful comments.