NOTE

Privacy and Criminal Certainty: A New Approach to the Application of the Private Search Doctrine to Electronic Storage Devices

Joseph Little[*]

TABLE OF CONTENTS

 J.D. Candidate, UC Davis School of Law, 2018; B.A. in psychology, Gonzaga University. Articles Editor, UC Davis Law Review. Thank you always to my friends and family for giving me the support to succeed in law school. This article would not have been possible without the inspiring commitment to privacy by Glenn Greenwald and others at The Intercept.

INTRODUCTION

Today's average electronic device stores more of an owner's personal information than ever before.[1] Tangentially, Americans are now overwhelmingly concerned with their privacy,[2] partially due to alarming revelations by whistleblowers, which have gathered significant media attention.[3] In fact, several prominent news outlets had previously called for President Obama to pardon Edward Snowden, perhaps the most well-known modern whistleblower.[4] This media attention has even transformed certain whistleblowers, including Snowden, into quasi-celebrities.[5] As privacy concerns are elevated into Americans' everyday thoughts, focus on courts' application of the Fourth Amendment is becoming increasingly important. Courts struggle to apply the Fourth Amendment's protections against unreasonable searches and seizures[6] to electronic storage devices.[7] Particularly, when private parties conduct searches of electronic devices and subsequently turn over the devices to law enforcement officers, courts face a difficult task in balancing the interests of law enforcement with the device owner's privacy.[8]

---

[1] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005).

[2] *See 2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition*, TRUSTARC, https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/ (last visited July 12, 2017) [hereinafter *Consumer Privacy Infographic*] (reporting that sixty-four percent of Americans think privacy should be a human right).

[3] *See* Dana Gold, *Snowden, Institutional Corruption & the "Vilified Whistleblower*," HARV. U. CTR. FOR ETHICS: BLOG (Oct. 17, 2014), https://ethics.harvard.edu/blog/snowden-institutional-corruption-%E2%80%9Cvilified-whistleblower%E2%80%9D (noting the wide public awareness generated by whistleblower Edward Snowden).

[4] *See, e.g.*, R. Kyle Alagood, *Obama Must Pardon Manning and Snowden Before Trump Takes Office*, CNN (Dec. 19, 2016, 8:57 AM), http://www.cnn.com/2016/12/19/opinions/pardon-manning-and-snowden-alagood-opinion/index.html; Kenneth Roth & Salil Shetty, *Pardon Edward Snowden*, N.Y. TIMES (Sept. 15, 2016), https://www.nytimes.com/2016/09/15/opinion/pardon-edward-snowden.html.

[5] At the time of this publication, Edward Snowden has amassed over three million followers on Twitter. Edward Snowden (@Snowden), TWITTER, https://twitter.com/snowden (last visited July 12, 2017).

[6] *See* U.S. CONST. amend. IV; *infra* Parts I.C–D.

[7] *See* Marc Palumbo, Note, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 979-80 (2009) (noting that courts use the Fourth Amendment to balance the privacy concerns of individuals against the needs of law enforcement officials).

[8] *See infra* Parts I.C–D. While whistleblowers like Snowden have highlighted different methods of privacy intrusions, the same privacy interests are at stake in the application of the Fourth Amendment to electronic storage devices. *See infra* Part I.B.

While the application of the "private search doctrine" to physical, non-electronic storage containers is settled,[9] the federal circuits have generally applied one of two approaches to electronic storage devices: the "Virtual File" approach or the "Physical Device" approach.[10] Although both of these approaches have their merits, the Virtual File approach unnecessarily restricts law enforcement efforts in conducting warrantless searches of these devices, while the Physical Device approach destroys a device owner's privacy.[11]

This Note argues that the current circuit split in applying the private search doctrine to electronic storage devices[12] should be resolved with a third approach: the "Organizational Unit" approach.[13] Generally, this approach would likely allow a law enforcement officer to replicate a search of the files that a private party has already searched, while also granting authority to extend that search, without a warrant, to other files contained within the same categorical unit of storage as the privately searched files. Part I discusses the background of the private search doctrine and the privacy interests at stake in searches of electronic storage devices.[14] Further, Part I summarizes the circuit decisions adopting the Virtual File and Physical Device approaches, while presenting the alternative Organizational Unit approach.[15] Part II argues that the approaches adopted by the various circuits do not effectively balance competing government and personal privacy interests.[16] Part II also argues that the Organizational Unit approach effectively balances these interests by adhering to the virtual certainty test established in *United States v. Jacobsen*[17] and providing law enforcement with a workable tool for conducting these searches that

[9] *See* Kerr, *supra* note 1, at 533 ("[T]he courts have developed clear rules to regulate the enter-and-retrieve mechanism of traditional physical searches.").

[10] *See infra* Parts I.C–D.

[11] *See infra* Part II.A.

[12] *See* Orin Kerr, *Eleventh Circuit Deepens the Circuit Split on Applying the Private Search Doctrine to Computers*, WASH. POST: THE VOLOKH CONSPIRACY (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/?utm_term=.9b603763d1bc (noting that the recently widened circuit split is "ripe for Supreme Court review").

[13] The "Organizational Unit" approach is untested but aims to strike a workable balance between other approaches.

[14] *See infra* Part I.

[15] *See id.*

[16] *See infra* Part II.

[17] 466 U.S. 109 (1984).

also protects personal privacy.[18] Finally, Part II summarizes why the Organizational Unit approach is the best application of the private search doctrine to warrantless searches of electronic devices.[19]

I. BACKGROUND

A. Private Search Doctrine

The Fourth Amendment prohibits unreasonable searches and seizures,[20] but this protection does not extend to searches conducted by private parties.[21] Under the "private search doctrine," a government search does not require a warrant when it follows, without exceeding, a private party's search.[22] The Fourth Amendment's conception of searches did not envision non-physical searches of electronic storage devices, and the current case law's "enter-and-retrieve" approach to physical searches does not suit non-physical searches.[23] While courts have long articulated rules for physical searches, these rules are not useful to law enforcement officers when searching electronic devices.[24]

Much of the current case law regarding the private search doctrine cites *United States v. Jacobsen*,[25] where the Court established the "virtual certainty" test for evaluating the actions of officers who replicate private searches of physical devices.[26] In *Jacobsen* employees of a private freight carrier examined a damaged parcel's contents and found plastic bags containing an unknown white powder.[27] The employees contacted the Drug Enforcement Agency, who, without a warrant, searched the parcel again and conducted a chemical test on the powder for cocaine.[28] The Supreme Court held that the officers did not exceed the scope of the private search by searching the parcel and conducting the cocaine test because the search and test did not

---

[18] *See infra* Part II.

[19] *See id.*

[20] U.S. CONST. amend. IV.

[21] *See* Walter v. United States, 447 U.S. 649, 656-57 (1980).

[22] *See id.*

[23] *See* Kerr, *supra* note 1, at 533.

[24] *See* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 113 (2011) ("Search and seizure law is heavily premised on physical facts: it governs what places officers can enter and what things they can seize, but not what information they may learn.").

[25] 466 U.S. 109 (1984).

[26] *See id.* at 119.

[27] *Id.* at 111.

[28] *Id.* at 111-12.

jeopardize privacy interests by revealing anything new.[29] Specifically, a positive test result would only confirm that the privately searched substance was contraband, while a negative test result would not have revealed any other information.[30] The Court reasoned that the officers had the authority to search the rest of the parcel, even though the private parties had not done so, because the officers had a "virtual certainty" that nothing else of significance was in the package.[31]

While *Jacobsen* provides a solid basis for further development of the private search doctrine, its virtual certainty test proves less helpful when applied to searches of electronic storage devices.[32] However, the test allows modern courts some flexibility in determining the bounds of a follow-up government search of an already privately searched device.[33]

B. Privacy Interests at Stake

As previously mentioned, most Americans are concerned with their right of privacy.[34] However, scholars have not reached a consensus on a coherent definition of privacy.[35] In *Whalen v. Roe*, the Court noted that "the individual interest in avoiding disclosure of personal matters" is a significant interest an individual has in privacy.[36] *Whalen* influenced many lower courts to recognize a constitutional right to privacy in this regard.[37] However, a more suitable definition of privacy in the modern age is one that incorporates protection of a person's

[29] *See id.* at 118-19.

[30] *See id.* at 123.

[31] *Id.* at 119.

[32] *See* Stephen LaBrecque, *"Virtual Certainty" in a Digital World: The Sixth Circuit's Application of the Private Search Doctrine to Digital Storage Devices in* United States v. Lichtenberger, 57 B.C. L. REV. E-SUPPLEMENT 177, 189 (2016).

[33] *See, e.g.*, *Jacobsen*, 466 U.S. at 119 (allowing officers to extend the scope of a private search so long as they had a virtual certainty of what an extension of that search would reveal).

[34] *See Consumer Privacy Infographic*, *supra* note 2. The right of privacy is not explicitly protected by the Constitution, yet still receives substantial protection from courts. *See* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 407 (2013) ("While there is not an explicit clause in the U.S. Constitution that states the existence of a general right to privacy, courts have held that such a right exists and is protected by the Constitution.").

[35] *See id.* at 377 (explaining that the lack of a coherent definition of privacy might be attributed to the use of the term in many "distinct but interrelated issues").

[36] *See* Whalen v. Roe, 429 U.S. 589, 599 (1977).

[37] *See* Kesan et al., *supra* note 34, at 407.

information from others' five senses *and* surveillance devices.[38] While the law is often slow to accommodate technological advances,[39] judges appear to be increasingly aware that electronic storage devices are inherently different from physical objects.[40] As electronic devices become more advanced and capable of enhancing nearly every aspect of our lives, they will inevitably possess the ability to reveal an alarming amount of a person's private information.[41] The Supreme Court has recently acknowledged this phenomenon, noting that modern cell phones are analogous to computers and contain an immense storage capacity, including a digital record of a person's personal and professional life.[42]

Law enforcement officers cannot apply the same methods and logic behind their searches of physical objects to electronic storage devices because they are inherently different.[43] This difference is partly because physical searches are much more expensive and time-pressured.[44] A data search is often only limited by the time that the officer is willing to devote to the case.[45] Further, the wealth of information that computers hold spans so many aspects of a person's life that a greater potential exists that a search will reveal private information unrelated to the purpose of the search.[46] As law enforcement agencies increase their use of digital evidence in the investigation and prosecution of crime,[47] it is important that they have

[38] Anita L. Allen, *Privacy-As-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 867 (2000).

[39] *See, e.g.*, Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology.

[40] *See* United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012) ("Judges are becoming aware that a computer . . . is not just another purse or address book.").

[41] *See* Kerr, *supra* note 1, at 569 ("[W]e may eventually approach a world in which a considerable chunk of our lives is recorded and stored in perpetuity in our computers.").

[42] Riley v. California, 134 S. Ct. 2473, 2489-91 (2014).

[43] *See* Kerr, *supra* note 1, at 569.

[44] *See, e.g.*, *id.*

[45] *See id.* at 569-70 (noting that invasive computer searches are "the norm rather than the exception").

[46] *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.").

[47] *See* Goldfoot, *supra* note 24, at 112-14 (noting common use of computer forensic examiners in criminal investigations).

a clear, workable framework to use when conducting these searches, so as to limit invasions of privacy.[48] The Supreme Court must resolve the current circuit split by establishing a workable rule for law enforcement that also protects the privacy of the twenty-first century consumer of digital storage devices and communication media.[49]

C. Decisions Adopting the Physical Device Approach

Circuits vary as to the extent a law enforcement officer may search an electronic storage device once a private party has searched at least some of the files on the device. Currently, the Fifth and Seventh Circuits apply the Physical Device approach.[50]

In *United States v. Runyan*, law enforcement officers conducted a warrantless search of a collection of disks that the defendant's wife turned over to the officers after she discovered child pornography on some of the disks.[51] The officers viewed the contents of each disk in the collection, including those that the wife had not searched.[52] The court held that the officers exceeded the scope of the wife's search by searching the disks that she had not searched herself.[53] However, the court ruled that the officers did not exceed the scope of the search when they viewed all the files on the disks that the wife had searched, even though she only viewed some of the files on those disks.[54] The court feared that requiring a warrant to view all the files on the disks would waste officers' time, especially when officers are misled about the incriminating content on a device.[55]

In *Rann v. Atchison*, the defendant's relatives searched the defendant's zip drive and digital camera memory card and then turned the devices over to law enforcement.[56] The relatives alleged that the

---

[48] *See* United States v. Lichtenberger, 786 F.3d 478, 483-84 (6th Cir. 2015) (addressing concerns that digital searches can accidentally reveal private information unrelated to the purpose of the search).

[49] *See* Palumbo, *supra* note 7, at 980 ("That the cases that have so far reached the federal courts have dealt almost exclusively with despicable actions should not serve as a bar to the development of Fourth Amendment doctrine that properly balances the privacy concerns of individuals against the needs of law enforcement officials moving forward.").

[50] *See* Rann v. Atchison, 689 F.3d 832, 836-37 (7th Cir. 2012); United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001).

[51] *See Runyan*, 275 F.3d at 453-54.

[52] *See id.*

[53] *See id.* at 464.

[54] *See id.* at 464-65.

[55] *See id.* at 465.

[56] *See* Rann v. Atchison, 689 F.3d 832, 834 (7th Cir. 2012).

devices contained child pornography.[57] The court held that the law enforcement officers had the authority to search the entirety of the devices without a warrant because the police were "substantially certain" that the devices contained child pornography.[58] In fact, the court authorized this extensive search without proof that the devices had actually been searched or even contained a single instance of child pornography.[59]

Essentially, the Physical Device approach adopted by *Rann* and *Runyan* gives law enforcement officers the authority to search each file, folder, and metadata contained within an electronic device, so long as a private party has searched a single file within that device.[60] Even if the private party does find criminal data, the Physical Device approach allows warrantless government intrusion into areas of a device that contain sensitive, personal, and non-criminal information that should require a properly-tailored warrant.[61] With privacy concerns on the rise,[62] it is alarming to see that multiple circuits have adopted this problematic approach.[63]

D. Decisions Adopting the Virtual File Approach

The Sixth and Eleventh Circuits, and arguably the Tenth Circuit, have instead adopted a Virtual File approach.[64] This approach is more restrictive of warrantless searches of electronic storage devices after a private party has already searched the device.[65]

In *United States v. Lichtenberger*, the defendant's girlfriend found dozens of child pornography images on his laptop and later showed a police officer a handful of those images.[66] The defendant stored the

---

[57] *See id.*

[58] *See id.* at 837-38.

[59] *See id.* at 834-38.

[60] *See generally id.* (holding that "the police search did not exceed or expand the scope of the initial private searches . . . ."); *Runyan*, 275 F.3d at 465 (holding 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 . . . .").

[61] *See generally Rann*, 689 F.3d 832.

[62] *See Consumer Privacy Infographic*, *supra* note 2.

[63] *See generally Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 449.

[64] *See* United States v. Ackerman, 831 F.3d 1292, 1306-09 (10th Cir. 2016); United States v. Johnson, 806 F.3d 1323, 1330-38 (11th Cir. 2015); United States v. Lichtenberger, 786 F.3d 478, 483-86 (6th Cir. 2015).

[65] *See* Steptoe & Johnson LLP, *Eleventh Circuit Limits Application of Private-Search Doctrine to Digital Data*, 884 E-COMMERCE LAW WEEK (Jan. 16, 2016), http://www.steptoe.com/publications-11021.html [hereinafter Steptoe & Johnson].

[66] *Lichtenberger*, 786 F.3d at 480-81.

images within several numerically labeled subfolders, all contained within a larger folder labeled "PRIVATE."[67] The defendant's girlfriend could not verify whether the images she showed law enforcement included any of the dozens of images she initially searched before contacting law enforcement.[68] The Sixth Circuit held that the police officer's second search, conducted in the girlfriend's presence, exceeded the scope of her initial search.[69] The prosecution could not prove that the images viewed in the second search were the same ones viewed in the girlfriend's initial search.[70] The court emphasized that the subfolders were labeled with numbers and not words and therefore could have contained "the most private sort" of information unrelated to the crime alleged, including bank statements, personal communications, and medical information.[71] In other words, there was a high probability that the search could have revealed the exact type of personal, non-criminal information upon which the *Jacobsen* Court sought to avoid intrusion.[72]

In *United States v. Johnson*, a store employee browsed defendant's cellphone and found pictures and videos of child pornography.[73] The employee showed the images to another employee in thumbnail format and only clicked a few of the images to expand them.[74] The second employee showed the images to an officer in thumbnail format and enlarged several of them.[75] The employee also showed the officer a video from the phone that depicted a girl eating ice cream.[76] Later, that officer showed another officer the images, the ice cream video, and a new video depicting child pornography that no private party had viewed before.[77] Police later obtained a warrant to search the rest of the phone.[78] The Eleventh Circuit held that the officer's review of the new video depicting child pornography exceeded the scope of the prior private search because no private party had viewed that specific

67 *Id.* at 481.

68 *Id.*

69 *Id.* at 491.

70 *See id.* at 490-91.

71 *Id.* at 489 ("The reality of modern data storage is that the possibilities are expansive.").

72 *See id.*

73 United States v. Johnson, 806 F.3d 1323, 1330-31 (11th Cir. 2015).

74 *Id.* at 1331.

75 *Id.*

76 *Id.*

77 *Id.* at 1331-32.

78 *Id.* at 1333.

video.[79] The court also implied that the officer did not exceed the scope of the private party's search by enlarging images that the private party previously viewed in thumbnail format only.[80]

In *United States v. Ackerman*,[81] after AOL's automatic scan of the email's hash value triggered an alert that one of the email's four attachments potentially contained child pornography, AOL forwarded an email and its attachments to a national clearinghouse, as required by law.[82] The clearinghouse opened the email and viewed each attachment, including those for which AOL's scan did not trigger an alert.[83] However, each of the attachments contained child pornography, so the clearinghouse alerted law enforcement that the defendant possessed child pornography.[84] The Tenth Circuit held that opening the email constituted a search, that the clearinghouse was operating as a government agent, and that opening the email exceeded AOL's search because AOL never opened the email itself.[85] The court refused to rule on whether the clearinghouse's search would have exceeded the scope of AOL's search if it had somehow, without opening the email, directly accessed the one attachment that triggered AOL's warning.[86] The court effectively held that a clearinghouse, operating as a government agent, may not open an email, even to view

[79] *See id.* at 1336.

[80] *See id.* ("Though [the officer] may have looked at some of the photos and the video more closely than did [the private party] . . . 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.").

[81] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016). A working knowledge of technical terms is critical to one's understanding of *Ackerman*. First, the documents or images attached within an email can be converted to a "hash value," which is a short string of characters generated by an algorithm in a way that makes it highly unlikely that another set of data will produce the same value. *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39-40 (2005). Second, certain email services use "hash value matching" to compare the hash values from outgoing emails with those contained within a database of known child pornography images. *Ackerman*, 831 F.3d at 1294. If the matching process reveals the potential presence of child pornography in an email, the law requires the service provider to report this information to law enforcement. *Id.* Given the fact that an algorithm generates a string of data to form a hash value, hash value matching is not analogous to actually opening an email and viewing its attachments. *See id.* at 1295.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *See id.* at 1301-07.

[86] *Id.* at 1306-07.

an attachment, simply based on a private party's scan of the hash value.[87]

Despite the court's refusal to elaborate on what the clearinghouse could have done to view the attachment without exceeding the scope of the private party's search, at least one prominent Fourth Amendment scholar, Orin Kerr, believes that the Tenth Circuit endorsed the Virtual File approach in *Ackerman*.[88] Kerr supports this belief by noting that the court refused to justify the clearinghouse's search under the private search doctrine when the clearinghouse actually opened the individual attachments while AOL did not.[89]

To summarize the Virtual File approach, law enforcement has the authority to conduct a warrantless search of any file that a private party has already searched.[90] An officer may not view any image, video, or document that a private party has not already viewed.[91] Technically, even if the private party viewed all but one image in a photo album and each image contained child pornography, an officer may not view the final image despite common sense indicating that the final image would almost certainly be child pornography.[92]

---

[87] *See id.*

[88] *See* Orin Kerr, *Tenth Circuit: Accessing Email Is a 'Search' Under the* Jones *Trespass Test*, WASH. POST: THE VOLOKH CONSPIRACY (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/?utm_term=.dd5482820ee8.

[89] *See id.* (implying that the court would have been endorsing the Physical Device approach had it allowed the clearinghouse to justify its actions under the private search doctrine since the results of the scan did indicate the presence of some illegal content).

[90] *See generally Ackerman*, 831 F.3d at 1292 (holding that the government clearinghouse exceeded the private search because the private part only hash-tagged the images, but did not view them); United States v. Johnson, 806 F.3d 1323 (11th Cir. 2015) (holding that an officer's viewing of a cellphone video exceeded the private search because the private party had not viewed it, but his viewing of images that the private party viewed only in thumbnail form was permissible); United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015) (holding that the officer's search exceeded the private search because the private party was not certain she had previously viewed the same photos).

[91] *See Lichtenberger*, 786 F.3d at 491 ("Officer Huston's warrantless review of Lichtenberger's laptop exceeded the scope of the private search Holmes had conducted earlier that day, and therefore violated Lichtenberger's Fourth Amendment rights . . . .").

[92] *See generally id.*

E. The Organizational Unit Approach

As an alternative to the Physical Device and Virtual File approaches, I propose the Organizational Unit approach, which falls somewhere in between the two. Under this approach, a law enforcement officer may replicate and slightly extend the search that a private party performed on an electronic storage device before obtaining a warrant. Specifically, an officer would have the authority to search each file located within a folder that contains at least one file that a private party has searched. For instance, if a private party viewed a single image in an album within a suspect's cell phone, an officer may view that image and any other image within that same album, without first obtaining a warrant. For a phone that organizes text messages in a chain between two or more parties, an officer may view the entire message chain, so long as a private party has read at least one message from the chain. Essentially, an officer may search the contents of whatever "organizational unit" a privately searched file is located within, be it an album, folder, message chain, or a single email with attachments. An officer may not cross organizational boundaries that would remove the search from the same unit or level of organization that the private party searched.

II. THE SUPREME COURT SHOULD REJECT THE VIRTUAL FILE AND PHYSICAL DEVICE APPROACHES IN FAVOR OF THE ORGANIZATIONAL UNIT APPROACH

A. Current Approaches Neglect Fourth Amendment Balancing of Competing Interests

The Supreme Court should not resolve the circuit split by adopting the Physical Device or Virtual File approaches advanced by either side of the split. Neither of these approaches remains true to the underlying policies of the Fourth Amendment and the private search doctrine.[93] Instead, the Court should adopt an approach that allows law enforcement officers to conduct their work and discover relevant incriminating information without risking suppression due to Fourth Amendment violations.[94] The Court must balance the interest in

[93] *See Lichtenberger*, 786 F.3d at 487 (recognizing that courts must balance the government's search interest against a defendant's privacy interest); Palumbo, *supra* note 7, at 994 (noting that courts use the Fourth Amendment to balance the privacy concerns of individuals against the needs of law enforcement officials).

[94] *See infra* Parts II.A.1–2 (arguing that the Virtual File and Physical Device approaches are inadequate because they ineffectively balance competing interests).

supporting officers' ability to conduct searches with individuals' right to privacy.[95] In fact, the Court should use its decision to signal a commitment to embracing the right to privacy in the midst of increased public concern.[96] Currently, neither side of the circuit split effectively balances government interests with individuals' privacy interests. Rather, each side embraces a policy extreme. The Physical Device approach grants too much leeway for the government to conduct warrantless searches,[97] and the Virtual File approach protects individuals' privacy to an absurd extent.[98] Alternatively, the Organizational Unit approach lies in the middle of these two extremes, achieving a more demonstrable balance between competing policies.

1. The Physical Device Approach Sacrifices Privacy

The Physical Device approach adopted by the Fifth and Seventh Circuits sacrifices too much privacy.[99] Under this approach, a law enforcement officer has the authority to conduct a warrantless search of an entire device simply because a private party viewed a single file or even part of a file.[100] The Physical Device approach likens an electronic device to a box, and the presence of anything criminal in the box justifies a warrantless search of the entire box.[101] However, an electronic storage device is hardly analogous to a physical container.[102] Laptops, phones, and other devices can hold much more data in a smaller space than any physical container, and therefore a search of an entire device is far more intrusive than a search of an entire

95 *See id.*

96 *See Consumer Privacy Infographic*, *supra* note 2.

97 *See* Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012); United States v. Runyan, 275 F.3d 449, 466 (5th Cir. 2001).

98 *See* United States v. Ackerman, 831 F.3d 1292, 1301-09 (10th Cir. 2016); United States v. Johnson, 806 F.3d 1323, 1335-37 (11th Cir. 2015); *Lichtenberger*, 786 F.3d at 487.

99 *See Lichtenberger*, 786 F.3d at 487 (recognizing that courts must balance the government's search interest against a defendant's privacy interest); Palumbo, *supra* note 7, at 994 (noting that courts use the Fourth Amendment to balance the privacy concerns of individuals against the needs of law enforcement officials).

100 *See supra* Part I.C.

101 *See Rann*, 689 F.3d at 836-37; *Runyan*, 275 F.3d at 458-63.

102 *See* United States v. Wicks, 73 M.J. 93, 102 (C.A.A.F. 2014) ("Because of the vast amount of data that can be stored and accessed, as well as the myriad ways they can be sorted, filed, and protected, it is not good enough to simply analogize a cell phone to a container.").

container.[103] In fact, more and more courts today criticize the concept of an electronic storage device as a physical container.[104]

If a private party searched part of a parcel and found contraband, the physical limits of the parcel dictate that searching its entirety will likely reveal additional contraband but little to no personal information.[105] However, the same logic does not apply to electronic storage devices.[106] The Physical Device approach ignores the storage capacities of modern electronic storage devices. For example, a hard drive can contain a vast amount of contraband among an even larger collection of personal data that is unrelated to criminal behavior.[107] Suppose one spouse searches the other spouse's laptop and showed police officers a file whose contents violated the law. Further, assume the file was stored within a folder labeled "PRIVATE." Surely the officers can view that file without a warrant under either of the current approaches.[108] However, under the Organizational Unit approach, they could view the rest of the folder containing that same file without a warrant, but not the entire laptop.[109]

The Physical Device approach runs afoul of privacy concerns. No matter how incriminating the contents of one folder may be, the law should not allow an officer to search an entire device without a warrant. Why allow a warrantless search of a folder entitled "Medical History" or "Family Reunion Photos" because a folder entitled "Private" contained incriminating content? Allowing such an extension of the search likens a computer to a box, which some experts predict could lead to "unpredictable, unstable, and even disturbing results."[110] This is needless infringement because electronic devices are nearly inseparable from our daily lives, storing more information and becoming increasingly ubiquitous with each technological advancement.[111] In sum, the Physical Device approach is an unacceptable abuse of privacy, giving law enforcement unjustified

---

[103] *See Lichtenberger*, 786 F.3d at 488 (citing the district court's finding that the search of a laptop is highly intrusive given the amount of data it can hold and therefore is not comparable to searching a physical container).

[104] *See, e.g.*, United States v. Crist, 627 F. Supp. 2d 575, 586 (M.D. Pa. 2008) (ruling that to view a hard drive as a physical container would impermissibly jeopardize privacy rights).

[105] *Cf.* United States v. Jacobsen, 466 U.S. 109, 119 (1984).

[106] *See Lichtenberger*, 786 F.3d at 487-88.

[107] *See id.* at 488-89.

[108] *See supra* Parts I.C–E.

[109] *See supra* Part I.E.

[110] *See* Kerr, *supra* note 1, at 556.

[111] *See id.*

discretion in how much personal information they can learn before obtaining a warrant.[112] The Physical Device approach is like an unwieldy paintbrush that allows law enforcement to paint alarmingly broad strokes in their warrantless searches.[113] However, the Virtual File approach is not an adequate alternative, more like an overly fine brush that covers too little ground for effective law enforcement.

2. The Virtual File Approach Is Too Difficult to Implement

The Virtual File approach adopted by the Sixth and Eleventh Circuits needlessly impedes government criminal justice efforts and presents workability issues.[114] While this approach is far more protective of privacy than the Physical Device approach, it is far more difficult to implement by law enforcement officers.[115] The Virtual File approach asks law enforcement to ignore impulses and common sense, limiting them to only the exact files that private parties have already viewed.[116]

In *Johnson*, for example, the court ruled that law enforcement exceeded the scope of the private party's search because they viewed a video on the cell phone that no private party had previously viewed.[117] While this error was ultimately harmless because law enforcement obtained a warrant on other grounds, the Virtual File approach would have resulted in the suppression of relevant evidence.[118] Despite the existence of at least one non-pornographic video in the album searched by the private party, the album contained such a large volume of child pornography that it functioned as a personal contraband storage unit.[119] If a private party showed officers a series of photographs from a phone's photo album and most, if not all, of the photos were contraband, common sense suggests that the remainder of the album would also be contraband.[120] Requiring a warrant to

[112] *See supra* Part I.C.

[113] *See id.*

[114] *See* Steptoe & Johnson, *supra* note 65.

[115] *See id.*

[116] *See supra* Part I.D.

[117] *See* United States v. Johnson, 806 F.3d 1323, 1336 (11th Cir. 2015).

[118] *See id.* at 1336-37.

[119] *See id.* at 1131-32 (describing the contents of the phone's media album, which contained a large amount of child pornography but also some non-pornographic images).

[120] *Cf.* United States v. Jacobsen, 466 U.S. 109, 119 (1984) (noting the virtual certainty that a package containing sealed contraband would not contain anything else of significance).

search the remainder of the album is akin to asking an officer to stop searching a suitcase utilized for drug trafficking, even though he is certain that he will find more drugs, simply because there may also be non-contraband within the suitcase.[121] Courts should not shield criminals from warrantless searches of electronic storage units simply because they chose to store some noncriminal data, whether intentionally or not, amidst their collection of contraband.[122]

Under the Organizational Unit approach, law enforcement in *Johnson* would have been able to continue to search the rest of the phone's album, a single organizational unit, without obtaining a warrant.[123] The fault lies on the defendant for failing to distinguish criminal and noncriminal data in the way he organized his data.[124] The court in *Johnson* erred by overemphasizing privacy and ignoring rational and workable means of weighing the government's criminal justice interests.

In *Lichtenberg* the prosecution was unable to prove which specific images the private party viewed.[125] Under these facts, the Physical Device approach would have allowed officers to tread over the right of privacy by embarking on a fishing expedition within the device.[126] However, it is equally unwise and an affront to common sense under the Virtual File approach to prevent officers from clicking a subsequent image or video contained within a single organizational unit.[127] Alternatively, under the Organizational Unit approach, where the prosecution could establish the identity of at least some of the images that the private party searched,[128] those images and others

---

[121] *Cf.* United States v. Bowman, 907 F.2d 63, 65 (8th Cir. 1990) (holding that once a private party opened a suitcase and a single bundle within it that contained cocaine, an officer had authority to open the rest of the suitcase's bundles despite not having a warrant).

[122] *Cf.* United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016); *Johnson*, 806 F.3d 1323; United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015).

[123] *Cf. Johnson*, 806 F.3d 1323 (holding that law enforcement exceeded the private party's search by viewing a video that no private party had viewed despite it being located in the same album as other files the private party viewed).

[124] *See id.* at 1331-32 (describing the organization of defendant's phone album, which included at least one non-pornographic video amongst other pornographic photos and videos).

[125] *See Lichtenberger*, 786 F.3d at 481.

[126] *Cf. supra* Parts I.C, II.A.1.

[127] *See* Steptoe & Johnson, *supra* note 65 (describing the inherent difficulty of the Virtual File approach).

[128] In *Lichtenberger*, the prosecution's inability to establish the identity of any of the images the private party had searched led to the evidence being inadmissible. *See Lichtenberger*, 786 F.3d at 481.

contained within the same folders would constitute valid evidence. In situations like *Lichtenberger*, the Organizational Unit approach strikes an appropriate balance between government and private interests, unlike the Virtual File approach.[129]

Advocates of the Virtual File approach might argue that even though the Organizational Unit approach protects privacy more than the Physical Device approach, it simply does not go far enough in preventing government intrusion into our personal lives.[130] However, in response, the Organizational Unit approach adequately protects privacy because it limits searches to how defendants choose to store their own information. The Virtual File approach protects privacy when there is no need to protect it. For instance, some psychologists believe that "humans have an innate desire to put things in order."[131] Since most electronic devices allow the user to organize data as they see fit, it is reasonable to assume that someone would keep similar files together on such a device.[132] Thus, someone seeking to store a criminal file would reasonably store them in the same digital organizational unit as other such files.[133] In fact, this is what happened in *Lichtenberger*, where the defendant kept all his criminal files together in subfolders within a larger folder labeled "PRIVATE."[134] Under the Organizational Unit approach, it is unlikely that the *Lichtenberger* court's fears of accidental discovery of significant personal information are credible.[135] If a private party shows a law enforcement officer a file or series of files, and the officer extends the search but stays within the same folder, the officer is unlikely to discover private information other than additional criminal data.[136] The possibility of an officer incidentally discovering other personal information is still present, but a defendant should not have an expectation of privacy when storing such personal information with

129 *See infra* Part II.C.

130 *See Lichtenberger*, 786 F.3d at 489 (warning that the warrantless search could have revealed non-criminal, personal information such as the defendant's bank records or medical history).

131 *See* Julie Beck, *The Existential Satisfaction of Things Fitting Perfectly into Other Things*, ATLANTIC (Aug. 14, 2015), http://www.theatlantic.com/health/archive/2015/08/the-existential-satisfaction-of-things-fitting-perfectly-into-other-things/401213.

132 *See, e.g.*, *Lichtenberger*, 786 F.3d at 481.

133 *Cf.* Beck, *supra* note 131 (stating that humans have an innate desire to, and derive pleasure from, organizing information categorically).

134 *See Lichtenberger*, 786 F.3d at 481.

135 *Cf. id.* at 489.

136 *Cf.* Beck, *supra* note 131.

incriminating information.[137] Thus, the Virtual File approach burdens law enforcement when there is no need to protect the privacy of incriminating information.

Imagine that an officer receives a cell phone confiscated by a private party. The party tells the officer that they looked at one image and believe it is child pornography. The officer would want to confirm the nature of the suspicious image before acting. Logically, the officer would click the next image within the same album or folder to confirm the suspicion before taking any action. Under the Virtual File approach, viewing any file that the private party had not viewed would require a warrant.[138] This approach asks officers to ignore their impulse to glance at data that the defendant chose to group with incriminating, privately searched data. Under the Organizational Unit approach, the officer could browse the rest of the phone's album to confirm his suspicions without having to seek a warrant.[139]

B. The Organizational Unit Approach Adheres to Jacobsen*'s Virtual Certainty*

Recall that in *Jacobsen*, the Supreme Court held that the law enforcement officer had authority to search the rest of a parcel that a private party had already searched because there was a virtual certainty that nothing else of significance was in the package.[140] While *Jacobsen* provides guidance on applying the private search doctrine in the physical world, the case can also help courts apply the doctrine in the context of electronic storage devices. While both sides of the circuit split have referenced *Jacobsen* in articulating their own approaches,[141] neither approach remains true to *Jacobsen* because both ineffectively balance private and governmental interests.[142]

As previously discussed, the Physical Device approach violates *Jacobsen* because it is inappropriate to treat electronic devices like physical containers due to the sheer amount of private information

---

[137] *See* United States v. Jacobsen, 466 U.S. 109, 119-21 (1984).

[138] *See supra* Part I.D.

[139] *See supra* Part I.E.

[140] *See Jacobsen*, 466 U.S. at 118-20.

[141] *See generally* United States v. Ackerman, 831 F.3d 1292, 1305-08 (10th Cir. 2016); United States v. Johnson, 806 F.3d 1323, 1338 (11th Cir. 2015); United States v. Lichtenberger, 786 F.3d 478, 481-90 (6th Cir. 2015); Rann v. Atchison, 689 F.3d 832, 836-37 (7th Cir. 2012); United States v. Runyan, 275 F.3d 449, 457-65 (5th Cir. 2001).

[142] *See supra* Part II.A.

they can store.[143] In the context of an entire electronic storage device, rarely, if ever, will a law enforcement officer be virtually certain that he will not discover anything else of significance beyond contraband.[144] However, the Virtual File approach also conflicts with *Jacobsen* because it assumes that law enforcement can never be virtually certain that they will find contraband by viewing additional files.[145] If *Jacobsen* applied the Virtual File approach, the officer would have violated the Fourth Amendment by searching the rest of the parcel, even though it was clear that the parcel entirely functioned as a drug trafficking storage unit.[146] *Jacobsen* indicates that the private search doctrine is supposed to assist law enforcement without infringing individual privacy.[147] However, the Virtual File approach's inherent workability issues do not provide such assistance.[148]

Alternatively, the Organizational Unit approach to the private search doctrine as applied to electronic storage devices conforms to *Jacobsen*.[149] First, imagine the parcel in *Jacobsen* is akin to a folder, album, or other unit of data organization of an electronic device.[150] Incriminating files stored with other contraband within a folder in an electronic device are like the bags of cocaine in *Jacobsen*.[151] Second, the entire electronic device itself is like the room where the freight employees discovered the damaged parcel in *Jacobsen*.[152] The law enforcement officers in *Jacobsen* did not have a virtual certainty that they would find only contraband if they opened other parcels in the room, even if they were from the same sender.[153] Likewise, an officer has no virtual certainty that if he leaves a computer folder containing illicit images that he will find illicit images by browsing other computer folders.[154]

---

143 *See supra* Part II.A.2.

144 *See id.*

145 *See supra* Part I.D.

146 *See* United States v. Jacobsen, 466 U.S. 109, 119 (1984) (holding that an officer did not need a warrant to continue a private party's search of part of a package when there was a virtual certainty that the package contained nothing else of significance).

147 *See id.* (noting that a follow-up search of a private party's search allows law enforcement to avoid the risk of the private party's flawed recollection of a search's findings).

148 *Cf.* Steptoe & Johnson, *supra* note 65.

149 *Cf. Jacobsen*, 466 U.S. 109.

150 *Cf. id.* at 111.

151 *Cf. id.*

152 *Cf. id.*

153 *Cf. id.*

154 *See, e.g.*, United States v. Lichtenberger, 786 F.3d 478, 489 (6th Cir. 2015)

Critics may disagree with this analogy, as a device may contain only private information belonging to one owner, while multiple parcels at a private freighter may belong to various owners.[155] Therefore, *Jacobsen* might allow an officer to search other parcels originating from the same sender based on the same virtual certainty of their contents.[156] However, it seems unlikely that the *Jacobsen* Court would have allowed this search, as it is possible that the sender could have sent personal packages that had nothing to do with drug trafficking, even if those packages were of similar weight and dimensions as the parcel that contained drugs.[157] Further, imagine law enforcement searching a hard drive with common ownership that organizes information according to different users. There would be no virtual certainty that folders belonging to different users would only contain contraband, and the Organizational Unit approach would not allow a search on those folders, recognizing that uncertainty.[158]

To discern how *Jacobsen* would apply in the electronic context, it is helpful to consider cases that relied on *Jacobsen* in the warrantless search of non-electronic, physical containers. In *United States v. Bowman*, an airline employee opened an unclaimed suitcase and found five identical bundles wrapped in towels and clothing.[159] The employee opened one bundle and found a white powdery substance.[160] He then contacted a federal narcotics agent, who identified the exposed bundle as cocaine and opened the other bundles, which also contained cocaine.[161] The court held that unwrapping the remaining identical bundles without a warrant was proper, reasoning that the presence of cocaine in the exposed bundle spoke volumes as to the contents of the remaining bundles to the trained eye of the officer.[162]

Here, the compartments of the suitcase are like a folder or album within an electronic device. Each unopened bundle resembles a

(addressing concerns that digital searches can accidentally reveal private information unrelated to the purpose of the search).

155 *Cf. Jacobsen*, 466 U.S. at 111 (describing a search conducted by private freighter employees of a single parcel originating from one sender).

156 *Cf. id.* at 119 (allowing an officer to extend a private party's search when the officer has a virtual certainty that he is unlikely to discover anything of significance beyond the contraband).

157 *Cf. id.* (holding that the officer had a virtual certainty that an extended search of a single parcel would reveal nothing else of significance).

158 *Cf. id.*

159 United States v. Bowman, 907 F.2d 63, 64 (8th Cir. 1990).

160 *Id.*

161 *Id.*

162 *Id.* at 65.

thumbnail of an unopened computer file. The airline employee effectively opened a single file contained in a single folder and found contraband. If there were multiple unclaimed suitcases, those would be comparable to other folders within a computer that a private party had not searched. Under the Organizational Unit approach, the agent would have the legal authority to open the rest of the bundles within the specific suitcase compartment (unit) without obtaining a warrant. Given the contents of one file contained within an organizational unit, there is a virtual certainty that the rest of the files in that organizational unit contain criminal information.

However, in the *Bowman* example, the officer would not have authority to open any other unclaimed suitcases without a warrant. Further, the suitcase itself is like an entire computer and each compartment within it is a folder. The agent may only search the compartment that contained the illicit bundles. The rest of the compartments, so long as they remain unopened by a private party, may have contained personal belongings and there would not be a virtual certainty that they contained contraband. In this case, the Virtual File approach would have limited the agent to only search the one bundle that the private party searched, while the Physical Device approach would have given the agent full discretion to open each compartment and arguably other unclaimed suitcases. Both of these results are unacceptable, and therefore extending *Bowman* and *Jacobsen* to electronic storage devices calls for the adoption of the Organizational Unit approach.

C. The Organizational Unit Approach Is Simple, Workable, and Preserves Privacy

Both the Physical Device and Virtual File approaches ineffectively balance policy concerns[163] and stray from the Supreme Court's virtual certainty approach in *Jacobsen*.[164] In contrast, the Organizational Unit approach remains true to *Jacobsen* by appropriately balancing private and governmental interests.[165] Still, a rule may be ideologically sound yet prove unworkable in practice.[166] However, as shown below, the Organizational Unit approach proves to be a common sense, workable

[163] *See supra* Part II.A.

[164] *See supra* Part II.B.

[165] *See supra* Parts II.A–B.

[166] *See, e.g.*, *supra* Part II.A.1.

method of conducting warrantless searches of electronic devices that private parties have already searched.[167]

Ideally, a government officer willing to conduct a search of an electronic device should have some working familiarity with how these devices generally store and organize information. The officer in *Lichtenberg* likely knew he was navigating different folders when he viewed different subfolders within the larger "PRIVATE" folder.[168] Going in and out of folders should have triggered the realization that he exceeded the scope of any folder the private party showed him.[169] Under the Organizational Unit approach, the officer could have taken note of which folders contained the images that the private party showed him, and he could have tailored the warrantless search to these folders without violating the defendant's Fourth Amendment rights. Further, if the officers in *Johnson* felt the temptation to enter the phone's text messages or internet browser to view the defendant's web history, the Organizational Unit approach would dissuade them from partaking in these breaches of privacy. The officers would know their limits, yet have flexibility in their search, and the defendant would not have to sacrifice any more privacy than necessary.

As with any approach, limiting the warrantless search to a single organizational unit presents some workability issues. For instance, imagine a scenario where a private party opens a file contained within a folder. The folder also contains a subfolder, but the private party did not open the subfolder. Under the Organizational Unit approach, a law enforcement officer is limited to searching each file contained within the larger folder but cannot open any files contained within the subfolder. In fact, this approach would not even allow him to open the subfolder without a warrant. Instead, a computer is more like a warehouse that holds a series of further containers, and the opening of each new folder is akin to opening a new container.[170] A law enforcement officer may not open an additional folder, even if contained within a privately searched folder, unless a private party has opened the folder itself.

Imagine that the private party opened the subfolder, but did not open any of its files. In that situation, the officer could also open the subfolder, essentially repeating the search, but could not open a single file. However, suppose the private party opened the subfolder, did not

---

167 *See supra* Part II.B.

168 *See* United States v. Lichtenberger, 786 F.3d 478, 488-89 (6th Cir. 2015).

169 *See id.* (noting that the private party could not verify if the officer viewed a single image that the private party viewed within the larger "PRIVATE" folder).

170 *See* Goldfoot, *supra* note 24, at 112-13.

open any of its files, but could tell from the thumbnails of the files that they contained contraband. In this situation, an officer should be able to open these same files without a warrant because the thumbnails would give the officer a virtual certainty of the files' contents.

A perceivable issue with the Organizational Unit approach is the risk of a private party changing the organization of a suspect's files. For instance, a private party could, intentionally or accidentally, move an illicit photo from one folder into another folder that contained no contraband. While the risk of private party reorganization is legitimate, the issue seems unlikely and too fact-specific to discuss at length in this paper. The most likely scenario in which a private party will move a suspect's files would be if the party reorganized all of a suspect's contraband data into a single location. In this situation, privacy risks are minimal since the private party would have effectively removed any contraband away from a suspect's private, non-criminal data. However, if a law enforcement officer has any doubts about whether or not someone has reorganized or tampered with a suspect's files, that officer should seek a warrant to avoid risking suppression of evidence.

CONCLUSION

For the reasons discussed above, the Supreme Court should resolve the current circuit split by explicitly rejecting the Physical Device and Virtual File approaches and adopting the Organizational Unit approach. The Physical Device approach sacrifices too much privacy, while the Virtual File approach presents workability issues and needlessly limits the scope of an officer's follow-up search. Further, both of these approaches stray from the virtual certainty test established in *Jacobsen*. The Organizational Unit approach presents a workable means for officers to conduct follow-up searches while remaining true to *Jacobsen*. Officers will have a virtual certainty that they will discover contraband if they remain within a single organizational unit. This approach appropriately balances government and personal privacy interests by giving officers the flexibility they need in conducting their duties, while also protecting private information from unnecessary exposure.