EMORY | LAW

Emory Law Journal

Volume 66 | Issue 2

2017

Lichtenberger, Sparks, and Wicks: The Future of the Private Search Doctrine

Alexandra Gioseffi

LICHTENBERGER, SPARKS, AND *WICKS*: THE FUTURE OF THE PRIVATE SEARCH DOCTRINE

ABSTRACT

Electronic devices are becoming increasingly prevalent in our daily lives, simultaneously replacing photo albums, address books, printed documents, and other, previously indispensable items. Electronic devices have even invaded a controversial area of Fourth Amendment jurisprudence: the private search doctrine. However, this doctrine's application to electronic devices suffered from a dearth of existing law. Courts sought to fill this gap using two primary approaches: the container approach and the particularity approach. The container approach ignores the modern realities of electronic devices and the related privacy concerns. In contrast, the particularity approach accommodates these contemporary realities and increased privacy interests. This Comment concludes that courts should adopt the particularity approach to protect individuals from invasive government searches, in the true spirit of the Fourth Amendment.

INTRODUCTION

The Supreme Court set the stage for modern Fourth Amendment analysis in the paramount electronic device case *Riley v. California*.[1] The Court observed that cell phones are now so commonplace that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[2] It is clear to see why the Court made such an observation, as electronic devices[3] are essentially extensions of their owners.[4] In addition to holding digital imprints of electronic device users' lives, in effect representing an annex of the memory, the Court noted that "more than 90% of American adults" have cell phones.[5] Thus, the vast majority of Americans uses electronic devices and inherently recognizes the convenience and power of these devices as the norm in our society.[6] However, the unique Fourth Amendment consequences associated with these devices are not as facially obvious.[7] The constitutional

---

[1] 134 S. Ct. 2473, 2484 (2014).

[2] *Id.* Other courts have also commented on the widespread use of cell phones and other technology. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring); United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015); *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1022 (N.D. Cal. 2015); United States v. Saboonchi, 990 F. Supp. 2d 536, 556 (D. Md. 2014); *In re* Malik J., 193 Cal. Rptr. 3d 370, 375 (Cal. Ct. App. 2015); State v. Andrews, 134 A.3d 324, 326 (Md. Ct. Spec. App. 2016); State v. Tate, 849 N.W.2d 798, 813–14 (Wis. 2014) (Abrahamson, C.J., dissenting).

[3] For the purposes of this Comment, "electronic devices" includes cell phones, tablets, computers, media storage devices, and other digital devices and technology.

[4] *See Riley*, 134 S. Ct. at 2490 ("[N]early three-quarters of smart phone users report being within five feet of their phones most of the time . . . ."); Tracey v. State, 152 So. 3d 504, 524 (Fla. 2014). Further, electronic devices are extensions of their users because people regularly store "a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Riley*, 134 S. Ct. at 2490; *see* Leanne Andersen, People v. Diaz*: Warrantless Searches of Cellular Phones, Stretching the Search Incident to Arrest Doctrine Beyond the Breaking Point*, 39 W. ST. U. L. REV. 33, 49 (2011) (explaining that electronic devices are "extension[s] of our own memory" (quoting United States v. Arnold, 454 F. Supp. 2d 999, 1000 (C.D. Cal. 2006))).

[5] *Riley*, 134 S. Ct. at 2490 (further explaining that "12% [of smart phone users admit] that they even use their phones in the shower," and that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time"); *see* Adrianna Patrina Agosta, Note, *The Law Catching Up with the Evolution of Cell Phones: Warrantless Searches of a Cell Phone are Unconstitutional Uunder the Fourth Amendment*, 92 U. DET. MERCY L. REV. 131, 131 (2015).

[6] *See Riley*, 134 S. Ct. at 2490. In addition, it is becoming rare to encounter someone who does not use an electronic device. *See id.*; *see also* Samuel J. H. Beutler, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest*, 15 VAND. J. ENT. & TECH. L. 375, 376 (2013) (providing statistics on the widespread use of cell phones).

[7] *See Riley*, 134 S. Ct. at 2489–91; *see also In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3rd Cir. 2010) ("[I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information.").

implications of this widespread technological phenomenon are at the heart of the *Riley* opinion and this Comment.

The *Riley* majority analyzed the constitutional impact of the electronic device era by identifying two inherent differences between electronic devices and other types of possessions.[8] First, the Court distinguished electronic devices based on the qualitative disparity between electronic devices and other items.[9] The Court's analysis of the quantitative inequality centered on the "immense storage capacit[ies]" of electronic devices.[10] In particular, the "immense storage capacit[ies]" of electronic devices far exceed the previous physical restrictions on what an individual could carry with them.[11] Smart phones in 2014 could store "millions of pages of text, thousands of pictures, or hundreds of videos."[12] In comparison, an individual would be hard pressed to carry around physical copies of that quantity.[13] Second, the Supreme Court noted that electronic devices present distinct Fourth Amendment issues to the extent that they are qualitatively different from other items.[14] Unlike other items, electronic devices concentrate various categories of personal information on one device, including "Internet search[es] and browsing history,"[15] location tracking data,[16] medical records,[17] and many other types of

---

[8] *Riley*, 134 S. Ct. at 2489 (explaining that cell phones are different from other objects "in both a quantitative and qualitative sense").

[9] *Id.* In particular, the Court identified four privacy issues that arise because of the quantitative differences between cellular phones and other types of objects: (1) cell phones have the potential to concentrate various types of data on one device, thereby forming a more complete look into the owners' lives than looking at each type of data independently; (2) the quantity of each type of data that can be stored on a cell phone means that "the sum of an individual's private life can be reconstructed"; (3) the data found on a cell phone can predate the cell phone itself, providing a historical record of the owners' lives; and (4) the "pervasiveness" of electronic devices means that the vast majority of Americans now carry "a digital record" of their lives by way of their cell phones, as opposed to the few that carried such personal records on their persons prior to the cell phone phenomenon. *Id.* at 2489–90.

[10] *Id.* at 2489; *see* Adam Lamparello & Charles E. MacLean, Riley v. California*: Privacy Still Matters, But How Much and in What Contexts?*, 27 REGENT U. L. REV. 25, 31–32 (2014).

[11] *Riley*, 134 S. Ct. at 2489 ("Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

[12] *Id.* A cell phone can store the digital equivalent of "four million pages of Microsoft Word documents." Charles E. MacLean, *But, Your Honor, A Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 41, 46 (2012).

[13] *Riley*, 134 S. Ct. at 2489 ("Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read . . . .").

[14] *Id.* at 2490; *see also* United States v. Wurie, 728 F.3d 1, 8 (1st Cir. 2013) ("[The information stored on a cell phone] is, by and large, of a highly personal nature . . . .").

[15] *Riley*, 134 S. Ct. at 2490 (stating such search history "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD").

personal information.[18] These features make electronic devices convenient and valuable to users, but they also implicate Fourth Amendment issues concerning the amount and types of data that searches of these devices may reveal.[19]

The unique nature of electronic devices has particular impact on one area of Fourth Amendment law: the private search doctrine. The private search doctrine provides that government agents may, without first obtaining a warrant, reproduce a search performed by a private individual.[20] However, courts faced abundant litigation regarding whether a subsequent government search exceeded the scope of an initial private search, even in the pre-electronic device context.[21] The distinctive characteristics of electronic devices create an additional challenge for courts determining the scope of private searches. Courts have developed two dominant approaches for confronting this challenge: the container approach and the particularity approach. This divergence has created a split among the circuits.

The Fifth and Seventh Circuits utilize the container approach, which analogizes technological devices to static closed containers such as suitcases, duffle bags, and camera cases.[22] The Fifth Circuit in *United States v. Runyan* and the Seventh Circuit in *Rann v. Atchison* analogized media disks to traditional containers and determined that "the police . . . did not exceed the scope of the private search if they examined more files on the privately-

---

[16] *See id.* The location tracking data alone represent another modern constitutional debate. *See* State v. Tate, 849 N.W.2d 798, 814 (Wis. 2014) ("The United States Supreme Court characterizes location data as 'qualitatively different' from physical records, noting that location data can 'reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.' The more precise the tracking, the greater the privacy concerns." (quoting *Riley*, 134 S. Ct. at 2490)).

[17] *See Riley*, 134 S. Ct. at 2490 (discussing search histories that could potentially reveal searches for medical symptoms and cell phone applications for medical conditions such as pregnancy and addiction); *Tate*, 849 N.W.2d at 814 (describing how the GPS features on cell phones can track users to "doctors' offices . . . AIDS treatments centers, abortion clinics" and more places that could reveal clues into the users' health).

[18] *Riley*, 134 S. Ct. at 2490 (stating that people store "a digital record of nearly every aspect of their lives—from the mundane to the intimate" on their cell phones).

[19] *See id.* at 2489–90; *see also* Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 DUKE J. CONST. L. & PUB. POL'Y 83, 90–91 (2014).

[20] Walter v. United States, 447 U.S. 649, 656 (1980); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 233 (2005) ("A government search that merely replicates a previous private one is not a 'search' within the meaning of the Fourth Amendment; rather, the Amendment applies only to the extent that the government has exceeded the scope of the private search.").

[21] *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 115 (1984); *Walter*, 447 U.S. at 657 (explaining that if the government's search exceeds the bounds of the private search, it is a separate search and the government is required to obtain a warrant or prove the search is necessary under another exigent circumstance).

[22] *See infra* notes 101–29 and accompanying text.

searched disks than [the private searchers] had."[23] The Fifth and Seventh Circuits' interpretations of the container approach define the scope so broadly that they permit intrusive government searches that far exceed the literal reach of the private search.

The Sixth Circuit, the Eleventh Circuit, and the U.S. Court of Appeals for the Armed Forces opt for the particularity approach, an approach specifically designed to accommodate the unique characteristics and privacy concerns of electronic devices.[24] The common thread among applications of the particularity approach is the conclusion that government searches of electronic devices should be narrowly tailored to the precise scope of the private search.[25] The Sixth Circuit in *United States v. Lichtenberger*, like the Supreme Court in *Riley*, emphasized the privacy concerns associated with electronic devices[26] and concluded that an officer exceeded the scope of the private search by viewing more images than the private searcher.[27] Similarly, in *United States v. Sparks*, the Eleventh Circuit determined that a government searcher exceeded the scope of the private search when he viewed a video that the private searcher had not viewed.[28] The U.S. Court of Appeals for the Armed Forces also applied the particularity approach in *United States v. Wicks* when it held that a subsequent government search should be limited to the specific text messages viewed during the private search.[29] These applications of the particularity approach refine the concept of scope and prevent unjustified invasions of privacy.

---

[23] United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001); *see also* Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012).

[24] *See infra* notes 140–214 and accompanying text.

[25] *See* Clancy, *supra* note 20, at 203 ("Moreover, Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers . . . ." (quoting People v. Gall, 30 P.3d 145, 162–65 (Colo. 2001) (en banc) (Martinez, J., dissenting))); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547–48 (2005) (referring to this narrow approach as the "exposure-based approach" and stating that "government agents may view only the information viewed by the private actor unless they first obtain a warrant").

[26] *Compare* Riley v. California, 134 S. Ct. 2473, 2489–91 (2014) (identifying the differences between cell phones and other objects and accompanying privacy concerns), *with* United States v. Lichtenberger, 786 F.3d 478, 487–88 (6th Cir. 2015) (finding that "the nature of the electronic device greatly increases the potential privacy interests at stake").

[27] *Lichtenberger*, 786 F.3d at 488–91.

[28] 806 F.3d 1323, 1336 (11th Cir. 2015).

[29] 73 M.J. 93, 100–01 (C.A.A.F. 2014) ("[T]he scope of the private search can be measured by what the private actor *actually* viewed as opposed to what the private actor had access to view.").

This Comment focuses on the two approaches mentioned briefly above and proceeds in five parts. Part I lays the foundation for contemporary application of the private search doctrine by discussing the history of the Fourth Amendment and the development of the private search doctrine. Part II discusses the Fifth Circuit's container approach, which analogizes electronic devices to static closed containers, thereby giving the government access to data outside the literal scope of the private search. Part III examines the approach adopted by the Sixth Circuit, the Eleventh Circuit, and the Court of Appeals for the Armed Forces—the particularity approach. The particularity approach is specifically tailored towards the complexities and capacities of electronic devices. Part IV argues that the particularity approach is the superior approach. Accordingly, the central recommendation of this Comment is that the particularity approach best accommodates the unique qualities of electronic devices in the private search doctrine context. Part V discusses the widespread implications of courts utilizing the particularity approach.

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

> 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.[30]

The current state of Fourth Amendment jurisprudence is best understood in its historical context.[31] Section A of this Part discusses the history of the Fourth Amendment. The Framers' goals and the historical climate at the time of the Fourth Amendment's inception lay the foundation for determining which approach should dominate today. Section B examines the foundational private search doctrine cases, *Walter v. United States*[32] and *United States v. Jacobsen*.[33] These cases demonstrate early applications of the private search doctrine that inform modern applications.

---

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

[31] *See* Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 974 (1997) ("[T]he history of the Fourth Amendment is . . . important to modern-day analysis . . . .").

[32] 447 U.S. 649, 656 (1980).

[33] 466 U.S. 109, 117 (1984).

A. The History of the Fourth Amendment

Understanding the Fourth Amendment and how it shapes contemporary private search doctrine is best achieved by considering the Framers' intent, relevant case law, and the text of the Fourth Amendment. This section addresses these factors in turn.

First, the Framers drafted the Fourth Amendment to remedy two injustices that were prevalent in Colonial America and England: general warrants and writs of assistance.[34] General warrants granted officers broad authority to enter private residences and conduct unrestricted searches for evidence to substantiate charges of libel against the homeowners.[35] Writs of assistance gave revenue officials the power to freely search *any* container they believed held "uncustomed goods."[36] The Framers drafted the Fourth Amendment as a method of exterminating such misuse of authority by providing "restraints on arbitrary governmental intrusions."[37]

Second, case law provides further insight into modern Fourth Amendment doctrine. The Supreme Court expanded on the Framers' efforts and imposed additional checks on government search and seizure power by way of the

---

[34] Steagald v. United States, 451 U.S. 204, 220 (1981); Payton v. New York, 445 U.S. 573, 608 (1980) (White, J., dissenting); Boyd v. United States, 116 U.S. 616, 625–27 (1886); *see also* Maclin, *supra* note 31, at 939–41; George C. Thomas III, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 TEX. TECH. L. REV. 199, 206 (2010). Professor Thomas Clancy discusses the various cases and circumstances that motivated John Adams to lead the drafting of the Fourth Amendment. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979 (2011).

[35] *See Steagald*, 451 U.S. at 220 ("The general warrant specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched."); *Payton*, 445 U.S. at 583; *Boyd*, 116 U.S. at 625–26. For an example of the general warrants used to find evidence of libel by searching houses and seizing papers, see Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 562–63 (1999).

[36] *Steagald*, 451 U.S. at 220 ("[T]he writs of assistance used in the Colonies noted only the object of the search—any uncustomed goods—and thus left customs officials completely free to search any place where they believed such goods might be."); *Payton*, 445 U.S. at 608 (White, J., dissenting) ("The writs did not specify where searches could occur . . . . In effect, the writs placed complete discretion in the hands of the executing officials."); Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 77–78 (1996); The Honorable M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave It Birth*, 85 N.Y.U. L. REV. 905, 907 (2010).

[37] Marshall v. Barlow's, Inc., 436 U.S. 307, 327 (1978) (Stevens, J., dissenting); *see also* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 669–71 (1995) (O'Connor, J., dissenting); State v. Ochoa, 792 N.W.2d 260, 272 (Iowa 2010). The Framers were most concerned with "overreaching warrants" and "abusive search[es]." United States v. Leon, 468 U.S. 897, 972 (1984) (Stevens, J., concurring in part and dissenting in part) (citing T. TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 41 (1969)).

exclusionary rule.[38] The exclusionary rule stipulates that evidence obtained in violation of a defendant's Fourth Amendment rights shall not be admitted in the prosecution's case in chief.[39] The Court later incorporated the exclusionary rule against the states and held, "all evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court."[40]

Third, the text of the Fourth Amendment is instrumental in understanding modern Fourth Amendment jurisprudence.[41] The text of the Fourth Amendment and court interpretation of that text further illustrates the effort to restrict government search and seizure power.

The first clause of the Fourth Amendment states, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[42] Government conduct amounts to a search under this clause "when an expectation of privacy that society is prepared to consider reasonable is infringed"[43] or when the conduct

---

[38] *See* Weeks v. United States, 232 U.S. 383, 392 (1914) ("[U]nlawful seizures . . . should find no sanction in the judgments of the courts . . . ."). The goal of the exclusionary rule was "to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures." United States v. Calandra, 414 U.S. 338, 347 (1974); *see also* Elkins v. United States, 364 U.S. 206, 217 (1960).

[39] *See Weeks*, 232 U.S. at 398; United States v. Weaver, 808 F.3d 26, 33 (D.C. Cir. 2015); *see also* Donald Dripps, *The Case for the Contingent Exclusionary Rule*, 38 AM. CRIM. L. REV. 1, 2 (2001). There are several exceptions to the exclusionary rule, including "the standing doctrine, the good-faith exception, and the impeachment exception." *Id.* (footnotes omitted).

[40] Mapp v. Ohio, 367 U.S. 643, 655 (1961); *see, e.g.*, Caver v. Kropp, 306 F. Supp. 1329, 1330 (E.D. Mich. 1969); State v. Macri, 178 A.2d 383, 387 (N.J. 1962); State v. Hart, 841 N.W.2d 735, 739 (N.D. 2014); Commonwealth v. Szukics, 243 A.2d 198, 200 (Pa. Super. Ct. 1968). The exclusionary rule also extends to evidence "found to be derivative of an illegality or 'fruit of the poisonous tree.'" Segura v. United States, 468 U.S. 796, 804 (1984); *see, e.g.*, Murray v. United States, 487 U.S. 533, 536–37 (1988); Oregon v. Elstad, 470 U.S. 298, 305–06 (1985); Nix v. Williams, 467 U.S. 431, 441 (1984).

[41] *But see* Thomas, *supra* note 34, at 199 ("Indeed, reading the text without the gloss supplied by history or the Court's doctrine reveals that it provides almost no guidance on any issue except the contents of a warrant.").

[42] U.S. CONST. amend. IV. (articulating the "Reasonableness Clause"); *see also* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 202 (1993).

[43] United States v. Jacobsen, 466 U.S. 109, 113 (1984). The test used to determine whether there was a reasonable expectation of privacy comes from Justice Harlan's widely-cited concurring opinion in *Katz v. United States*. 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Justice Harlan's test has two requirements, a subjective requirement and an objective requirement. *Id.* There must be "an actual (subjective) expectation of privacy" and it must be one "that society is prepared to recognize as 'reasonable.'" *Id.* However, the *Katz* test is frequently "criticized as circular, and hence subjective and unpredictable." Kyllo v. United States, 533 U.S. 27, 34 (2001); *see also* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (describing the *Katz* test as "notoriously unhelpful").

at issue constitutes a trespass.[44] A "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[45] Notably, both these definitions include preservation of privacy or possessory interests and protection against intrusive government interference with those interests. Safeguarding these interests from government intrusion is a central tenet of Fourth Amendment doctrine, particularly in the context of electronic devices, where privacy interests are heightened.[46]

The remainder of the Fourth Amendment, called the "Warrant Clause," requires that warrants specify the places and things to be searched and seized.[47] The Warrant Clause prohibits "the seizure of one thing under a warrant describing another," effectively outlawing the general warrants that prompted the drafting of the Fourth Amendment.[48] The Supreme Court promotes the goals of the Warrant Clause and further limits government search and seizure discretion by consistently holding that warrantless searches and seizures "are *per se* unreasonable under the Fourth Amendment," unless they fall under an exception, including "special needs" and "exigent circumstances."[49] Accordingly, a government official is required to obtain a warrant before conducting a search, barring any exception.[50] This Comment focuses on instances of warrantless searches performed under the guise of one such exception, the private search doctrine.

---

[44] *See* United States v. Jones, 132 S. Ct. 945, 949–52 (2012). Fourth Amendment law was traditionally centered on the common law trespass doctrine. *Id.* at 949. However, the *Katz* expectation of privacy test was "*added to*, not *substituted for*, the common-law trespassory test." *Id.* at 952.

[45] *Jacobsen*, 466 U.S. at 113.

[46] *See* United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012).

[47] *See* U.S. CONST. amend. IV; *see also* Maclin, *supra* note 42, at 202.

[48] Marron v. United States, 275 U.S. 192, 195–96 (1927).

[49] City of Ontario v. Quon, 560 U.S. 746, 760 (2010); O'Connor v. Ortega, 480 U.S. 709, 732 (1987) (Scalia, J., concurring); Katz v. United States, 389 U.S. 347, 355–57 (1967). The Court has articulated many exceptions, ranging from emergency situations to plain view. *See* Kentucky v. King, 563 U.S. 452, 462 (2011) (stating that officers can conduct warrantless searches if the search is necessary "to prevent the destruction of evidence"); Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[L]aw enforcement officers may enter a home without a warrant to render emergency assistance to an injured occupant or to protect an occupant from imminent injury."); Michigan v. Tyler, 436 U.S. 499, 509 (1978) (holding that firefighters may enter a burning building to put out the fire and, once inside, "may seize evidence of arson that is in plain view" without violating the Fourth Amendment); United States v. Santana, 427 U.S. 38, 42–43 (1976) (explaining that a "hot pursuit" is an exigent circumstance that justifies a warrantless entry); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (defining the "plain view doctrine" as "under certain circumstances the police may seize evidence in plain view without a warrant"). Warrantless searches may also be conducted pursuant to valid consent, subject to the scope of that consent. Florida v. Jimeno, 500 U.S. 248, 252 (1991); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[50] *Coolidge*, 403 U.S. at 454–55.

B. The History of the Private Search Doctrine

The private search doctrine—and the circuit split regarding its application to electronic devices—is at the heart of this Comment. This section discusses the private search doctrine by examining private versus government action and two influential private search doctrine cases: *Walter v. United States*[51] and *Unites States v. Jacobsen*.[52]

First, the private search doctrine stems from the distinction between private and government action. Private and government action are divorced under the Fourth Amendment, as the Fourth Amendment applies only to state action.[53] Accordingly, "a private individual not acting as an agent of the Government or with the participation or knowledge of any government official" is not subject to the restrictions of the Fourth Amendment and may conduct an unreasonable search without violating the Fourth Amendment.[54]

The Supreme Court echoed this division between private and government action and set the foundation for contemporary private search doctrine in *Walter v. United States*.[55] In this seminal case, a private carrier mistakenly delivered several packages to the wrong recipient.[56] Employees opened the packages and discovered boxes of film with "suggestive" labels.[57] After seeing the labels, one of the employees removed a filmstrip and attempted to view it by holding it up to the light.[58] The employees then called FBI agents to the scene, and the agents subsequently viewed the film on a projector without obtaining a warrant.[59] The Supreme Court first addressed the initial search conducted by the employees and cited the Fourth Amendment's exclusion of private action.[60] "[A] wrongful search or seizure conducted by a private party

---

51 447 U.S. 649 (1980).

52 466 U.S. 109 (1984).

53 *See Walter*, 447 U.S. at 662 (Blackmun, J., dissenting); Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

54 *Walter*, 447 U.S. at 662 (Blackmun, J., dissenting); *see also Jacobsen*, 466 U.S. at 113. However, the private individual may face other causes of action for such an unreasonable search. *See* United States v. Koenig, 856 F.2d 843, 852 n.10 (7th Cir. 1988) ("The private actor's search may be limited by criminal law, by tort law, or by market forces . . . but not by the Constitution."). The Fourth Amendment does regulate the actions of government agents—those acting as "instruments" of the government at the time of the search. *Coolidge*, 403 U.S. at 487.

55 447 U.S. at 656.

56 *Id.* at 651.

57 *Id.* at 651–52.

58 *Id.* at 652.

59 *Id.*

60 *Id.* at 656.

does not violate the Fourth Amendment . . . ."[61] The Court then analyzed the subsequent FBI search and, in so doing, established the private search doctrine.[62] Pursuant to the private search doctrine, the Court determined that government officials may recreate the private search without obtaining a warrant; however, the warrantless government search cannot exceed the limits of the initial private search.[63]

The *Walter* decision set the stage for the modern application of the private search doctrine by emphasizing two factors: the privacy interests at stake and the scope of the initial private search.[64] The Court stressed the intent of the Framers to protect "unfrustrated" privacy interests and guard against broad, "indiscriminate searches and seizures."[65] In accordance with this intent, the Court applied a narrow scope and stated that the private searchers frustrated, but did not completely destroy, the expectation of privacy in the film when they opened the box and attempted to view one of the filmstrips.[66] Some Fourth Amendment-protected expectation of privacy remained, and the warrantless government search invaded that "unfrustrated" expectation of privacy.[67] In particular, "[t]he projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search."[68] In addition, the private search analysis in *Walter* is consistent with the particularity requirement found in the Warrant Clause of the Fourth Amendment.[69] "If a properly authorized official search is limited by the particular terms of its authorization, at least the same kind of strict limitation must be applied to any official use of a private party's invasion of another person's privacy."[70]

---

61 *Id.*

62 *Id.* at 656–57.

63 *Id.* (explaining that if the Government's search surpasses the limits of the private search, it is considered a separate, independent search).

64 *See id.* at 657–59.

65 *Id.* (citing Payton v. New York, 445 U.S. 573, 583 (1980)).

66 *Id.* at 659; *see also* Lynn M. Gagel, *Stealthy Encroachments Upon the Fourth Amendment: Constitutional Constraints and Their Applicability to the Long Arm of Ohio's Private Security Forces*, 63 U. CIN. L. REV. 1807, 1825 (1995) ("A government search following a private invasion is only justifiable—or authorized—because the private party has thwarted any privacy interest of the party being searched.").

67 *See Walter*, 447 U.S. at 659.

68 *Id.* at 657; *see also* Gagel, *supra* note 66, at 1825 ("The Court concluded that if the government overreaches the bounds of the initial private party search . . . it oversteps its initial authorization and, without additional justification, violates the Fourth Amendment.").

69 *See Walter*, 447 U.S. at 657 (stating that "[the Fourth] Amendment requires that the scope of every authorized search be particularly described"); *see also* U.S. CONST. amend. IV.

70 *Walter*, 447 U.S. at 657.

Four years later, in *United States v. Jacobsen*, the Court revisited the private search doctrine.[71] Employees for a private carrier were inspecting a cardboard box for damage when they discovered a tube made of duct tape.[72] The employees slit open the tube and observed several plastic bags containing a white, powdery substance.[73] The employees placed the plastic bags and the tube back into the cardboard box and notified the DEA.[74] Without first obtaining a warrant, a DEA agent removed the plastic bags from the previously cut-open tube, opened each of the bags, and conducted a field test to confirm that the powder was cocaine.[75]

First, the Court addressed the initial private search conducted by the employees and found that the Fourth Amendment's inapplicability to private action extended to the search conducted by the employees in the instant case.[76] Then, the Court analyzed the subsequent government search to determine whether the government search infringed upon any expectation of privacy that was not frustrated by the private search.[77] To reach its determination, the Court stated that government searches pursuant to the private search doctrine "must be tested by the degree to which they exceeded the scope of the private search."[78] Specifically, government officials violate the Fourth Amendment if they expand the scope of the government search to include items with an unfrustrated expectation of privacy.[79] The Court applied this rule to the circumstances of the case and determined that the employees frustrated the privacy interest in the contents of the package when they cut open the tube, removed the plastic bags, and called the DEA.[80] Thus, the agent did not infringe upon any unfrustrated privacy interest when he removed the bags from

---

[71] 466 U.S. 109, 115–18 (1984).

[72] *Id.* at 111.

[73] *Id.*

[74] *Id.*

[75] *Id.* at 111–12.

[76] *Id.* at 114–15 ("Whether [the initial invasions by the employees] were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character." (footnote omitted)).

[77] *See id.* at 115–18 (explaining that if someone exposes private information to a third party, his expectation of privacy in that information is frustrated and the government may use that "now nonprivate information" without obtaining a warrant, but if the expectation of privacy has not been frustrated in some information, the government may not use that information without obtaining a warrant).

[78] *Id.* at 115–17 (explaining that this rule stems from the rule that when "frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit government use of the now nonprivate information").

[79] *See id.* at 117 ("The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.").

[80] *Id.* at 119.

the tube.[81] The Court also considered what information the agent stood to gain from the re-examination and concluded that the agent was not poised to discover anything he did not already know.[82] For the preceding reasons, the Court concluded that the government agent did not exceed the scope of the private search, nor did the government search violate the Fourth Amendment.[83]

Both *Walter* and *Jacobsen* highlight the scope of the initial private search. However, determining the scope of private searches in the context of twenty-first century technology has proven controversial.[84] The remainder of this Comment surveys and assesses two dominant approaches that courts utilize in determining the scope of private searches of electronic devices.

II. THE CONTAINER APPROACH

Some courts apply traditional private search doctrine rules—typically used in the context of static containers—to private searches of electronic devices, in an approach this Comment refers to as the "container approach." Section A introduces the container approach. Section B details the Fifth Circuit's application of the container approach. Section C describes the Seventh Circuit's application of the container approach.

A. Description of the Container Approach

"[A] 'container' has been defined as 'any object capable of holding another object.'"[85] Due to the dearth in case law and the unresolved questions relating to the scope of a private search involving electronic devices,[86] courts adopting the container approach attempt to incorporate technology under the broad umbrella of this container definition. These courts thereby endeavor to

---

[81] *Id.* at 119–20.

[82] *Id.* at 120 (explaining that the agent did not learn anything from the government search that "had not previously been learned during the private search").

[83] *Id.* ("It infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment.").

[84] *Compare* United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (acknowledging that laptops are intrinsically different from standard containers), *and* United States v. Wicks, 73 M.J. 93, 102 (C.A.A.F. 2014) (differentiating cell phones from "static storage containers" because of the likelihood of "vast amount[s] of personal data" stored on cell phones), *with* United States v. Runyan, 275 F.3d 449, 462–64 (5th Cir. 2001) (treating computer disks as standard containers and using container case law to address the private search of computer disks).

[85] People v. Michael E., 178 Cal. Rptr. 3d 467, 479 (Cal. Ct. App. 2014) (quoting Riley v. California, 134 S. Ct. 2473, 2491 (2014)).

[86] *See also* Clancy, *supra* note 20, at 236–40 (stating that the issue of scope of a private search involving computers has resulted in "contradictory results").

streamline the issue of scope for private searches involving electronic devices, which the historical framework of the private search doctrine left open to "questionable results."[87]

Courts applying the container approach draw parallels between electronic devices—which they argue are just digital containers—and conventional closed containers at the heart of historical private search jurisprudence.[88] One traditional container rule frequently used in these analogies gives government officials broad authority to view all of the contents of a container if a private searcher merely opens that container.[89] This rule is justified on the basis of the subsequent government merely being more "thorough"; thus, a government search "[does] not exceed the scope of the prior private searches for Fourth Amendment purposes simply because they took more time and were more thorough than the [private searchers]."[90]

Courts have also addressed the question of scope in traditional private search cases involving multiple containers.[91] One such case determined that an officer exceeds the scope of the private search if he opens a separate, unopened container found inside a larger container that the private searcher did open.[92] Other cases involve identical closed packages, at least one of which the private searcher opened.[93] In such cases, government agents may open any identical

---

[87] *See id.* at 233 (stating that the private search doctrine left a gap when it came to computers and that "[t]he application of [the private search doctrine] in the computer context has sometimes led to questionable results"). Courts using the container approach seek to fill this void using an analogy to containers and existing rules. However, this Comment argues that this approach still results in "questionable" outcomes.

[88] Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012) (relying on the *Runyan* decision to analyze the private search of media devices under traditional container theories); United States v. Runyan, 275 F.3d 449, 462–64 (5th Cir. 2001) (applying container case law to computer disks). There are many private search doctrine cases involving containers for container approach supporters to rely upon in their analogies. *See, e.g.*, United States v. Oliver, 630 F.3d 397, 406–08 (5th Cir. 2011); United States v. Donnes, 947 F.2d 1430, 1439 (10th Cir. 1991); United States v. Bowman, 907 F.2d 63, 65 (8th Cir. 1990); United States v. Gricco, No. CR.A. 01-90, 2002 WL 393115, at *11 (E.D. Pa. Mar. 12, 2002).

[89] *See Gricco*, 2002 WL 393115, at *10–11 (holding that the government search of all the items in a container does not exceed the scope of the private search where the private searcher merely opened the trunk and saw guns). This rule is also consistent with the holding of static container case *Jacobsen*, which stated that government officials may conduct a warrantless search of a container in which the privacy interest has already been frustrated when a private searcher opened the container. *See* United States v. Jacobsen, 466 U.S. 109, 115–17 (1984).

[90] United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990).

[91] *See, e.g.*, *Oliver*, 630 F.3d at 408; *Donnes*, 947 F.2d at 1439; *Bowman*, 907 F.2d at 65.

[92] *See Donnes*, 947 F.2d at 1439 (holding that "by removing the lens case from the glove, and then opening the lens case, the officer exceeded the scope of the private search").

[93] *See, e.g.*, *Bowman*, 907 F.2d at 65.

bundles if factors render the contents of the identical bundles obvious.[94] These factors include whether there are any identifying indicators on the outside of the container, whether there is any information that could hint at the contents, and whether the government officials' experience provides insight into the contents.[95] For example, the Fifth Circuit applied these factors to an unsearched notebook inside an opened container.[96] The court concluded that an identifying label on the cover of the notebook, a protruding piece of paper, and the government officials' training rendered the contents of the notebook "obvious."[97] Because the contents were "obvious," the court held that the government officials did not conduct a separate, unconstitutional search in violation of the Fourth Amendment.[98]

Courts employing the container approach implement these and other traditional private search doctrine standards in the context of technology by likening electronic devices to closed containers.[99] The container approach, in effect, suggests that this direct analogy belies any notion that these devices require a specialized approach.[100] However, while the container approach successfully simplifies the task of determining the private search doctrine's scope for electronic devices, it also minimizes the unique privacy concerns associated with technology and permits exceedingly intrusive government searches.

---

94 *See id.* ("The presence of the cocaine in the exposed bundle 'spoke volumes as to [the] contents [of the remaining bundles]—particularly to the trained eye of the officer.'" (quoting United States v. Jacobsen, 466 U.S. 109, 121 (1984)).

95 *See Oliver*, 630 F.3d at 408.

96 *See id.* (explaining that the unsearched notebook was found within a box that a private searcher opened).

97 *Id.*

98 *Id.* ("Because the notebook's contents were obvious, agents did not exceed the scope of [the private searcher's] private search.").

99 *See* United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001) (analyzing the computer disks under traditional static container case law because neither side contested the point).

100 The container analogy suggests that rules for traditional containers are just as applicable to electronic devices. *See also* Clancy, *supra* note 20, at 195–96 (suggesting that "computers are containers" and that "the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers"). It should be noted that Professor Clancy rejects a "special approach" and advocates for a specific container analogy in the private search context—an analogy between computers and filing cabinets. *Id.* at 240 ("If computers are containers that hold various forms of information, then there is no principled distinction between them and a metal filing cabinet when applying the private search doctrine. That is to say that the rules regulating containers in the bricks and mortar world have equal applicability to computer searches.").

B. The Fifth Circuit's Application of the Container Approach

The Fifth Circuit applied the container approach in *United States v. Runyan*.[101] The search at issue in *Runyan* involved two private searchers and numerous media storage devices.[102] The first private searcher entered the defendant's property to retrieve some of her items but, instead, removed a duffle bag containing pornography and several media storage disks.[103] She and several friends later returned to the defendant's property and took a computer, floppy disks, CDs, and ZIP drives.[104]

The second private searcher searched about *twenty* of the CDs and floppy disks but *none of the ZIP drives*.[105] Her private search revealed images of child pornography, so she handed over to the police more than *forty* CDs, floppy disks, and ZIP drives.[106] Notably, she gave the police significantly more disks than she opened in her private search.[107] The first private searcher later gave the police additional CDs, the black duffle bag, the computer, and other items found on the defendant's property.[108]

A government agent viewed images from *every* CD, floppy disk, and ZIP drive received from the two private searchers.[109] Only then did he apply for warrants to search the computer, the disks, and the defendant's property.[110] A judge granted the warrants, and the defendant was subsequently indicted.[111] The defendant moved to suppress the evidence on the basis that the government agent violated his Fourth Amendment rights by searching all of

---

[101] *See* 275 F.3d at 463–65. It is important to note that the court utilized the container approach "[b]ecause neither party contest[ed] this point." *Id.* at 458 ("The government concedes that the disks found in the office near the computer are 'containers' and that the standards governing closed container searches are applicable."). Despite the Fifth Circuit's "assum[ing] without deciding" status, this Comment will reference the Fifth Circuit's utilization of the container approach, as is consistent with the opinion's treatment of disks as containers. *Id.*

[102] *Id.* at 453.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.* (stating that she viewed approximately twenty of the CDs and floppy disks but turned over to the police over forty CDs, ZIP disks, and floppy disks).

[108] *Id.*

[109] *Id.* at 454.

[110] *Id.*

[111] *Id.* at 455.

the disks, but the trial court denied the motion.[112] The defendant was convicted and appealed his convictions to the Fifth Circuit Court of Appeals.[113]

On appeal, the Fifth Circuit Court utilized the container approach to determine whether the government search exceeded the scope of the private search.[114] In applying the container approach, the *Runyan* court categorized the evidence into two classes: (1) the disks that were not opened during the private search, and (2) the images that were not viewed but that were on disks opened during the private search.[115]

The court first focused on disks that the private searchers did not open.[116] In keeping with the container approach, the court applied a standard typically used in the context of traditional containers to the media disks at issue in *Runyan*.[117] This standard states that a government search of a closed container does not constitute a separate search if the government officials are "substantially certain" of its contents.[118] The court applied this traditional standard to the disks at issue and determined that the government officials were not "substantially certain" of the contents of the disks that were not opened during the private search.[119]

Next, the court considered whether the government officials exceeded the scope when they viewed more images on each disk than the private

---

[112] *Id.*

[113] *Id.*

[114] *See id.* at 462–65; Benjamin Holley, Note, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 695 (2010) ("[The Fifth Circuit Court of Appeals] applied the closed-container analogy to digital storage.").

[115] *Runyan*, 275 F.3d at 461. The court addressed three issues: (1) whether the government search of disks that were not opened during the private search but that were similar to those opened during the private search exceeds the scope of the private search; (2) whether the government search of more images on a disk than the private searcher viewed exceeds the scope of the private search; and (3) whether government searchers' identification of the person in an image that the private searchers could not identify exceeds the scope of the private search. *Id.* at 461–62. However, only the first two prongs of the court's analysis are relevant to the scope of this Comment—the private search doctrine as it relates to electronic devices and technology.

[116] *Id.* at 462.

[117] *Id.* at 463–64 ("[T]he police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers unless the police are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise.").

[118] *Id.* at 463. If the contents of a container are obvious, then the expectation of privacy is frustrated. *See id.* at 463–64.

[119] *Id.* at 464 (explaining that the police could not have known the contents because there were no identifying labels and the private searcher testified that she did not know what was on the disks that she did not open).

searchers.[120] In its analysis, the court utilized a traditional container rule, which provides that a more thorough government search does not exceed the scope of the private search.[121] The Fifth Circuit Court expanded this traditional container proposition to media disks and likened each disk to a closed container.[122] Thus, the government's search of additional images on each disk was merely more thorough and did not exceed the scope of the private searches because the expectation of privacy in all the contents of the disks was frustrated when the private searchers merely opened the disks.[123]

By means of the two-pronged analysis discussed above, the *Runyan* court applied the container approach.[124] *Runyan* proposes that constitutional subsequent government searches cannot extend to unopened electronic devices but may cover more files on opened devices.[125] By allowing government searchers to warrantlessly access all of the data on a device that was only partially searched by a private individual, this case demonstrates the permissive government intrusions endorsed by the container approach. Further, the government search far exceeded the literal scope of the private search by including files that the private searchers did not open. Applying this holding to searches of cell phones or computers, it follows that government searchers can warrantlessly search all the content on that device where the private searcher merely opens one file on the device. This type of government intrusion is reminiscent of the broad searches that the Framers intended to eradicate by drafting the Fourth Amendment.

C. The Seventh Circuit's Application of the Container Approach

The Seventh Circuit mimicked the permissive searches allowed in *Runyan* in a case involving the private search of images on a camera memory card and a ZIP drive.[126] In *Rann v. Atchison*, the court adopted the Fifth Circuit's container approach and held that, "even if the police more thoroughly searched

---

120 *Id.*

121 *Id.* ("[T]he police do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties."). This analysis is consistent with the *Jacobsen* Court's finding that once a private searcher opened the tube, the expectation of privacy in the contents of that tube was frustrated. *See* 466 U.S. 109, 119–20 (1984).

122 *See Runyan*, 275 F.3d at 464–65.

123 *See id.* ("Thus, the police do not engage in a new 'search' for Fourth Amendment purposes each time they examine a particular item found within the container.").

124 *See id.* at 462–65.

125 *See id.*

126 *See* Rann v. Atchison, 689 F.3d 832, 834, 838 (7th Cir. 2012).

the digital media devices than [the private searchers] did and viewed images that [the private searchers] had not viewed, per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches."[127] The court also applied the "substantially certain" test, which was arguably an application of circular logic, and concluded that the government searchers were "substantially certain" of the contents of the disks because the private searchers knew the contents; therefore, the government searchers did not violate the Fourth Amendment.[128] Further, the court stressed the policy implications of the *Runyan* container approach decision—"[The *Runyan* decision] 'is sensible because it preserves the competing objectives underlying the Fourth Amendment's protections against warrantless police searches.'"[129] Despite this argued rationale for the container approach, allowing broad, expansive searches of electronic devices implicates dangers that cannot be justified under the Fourth Amendment.

III. THE PARTICULARITY APPROACH

Alternatively, some courts challenged with interpreting the scope of a private search in the technology era apply what this Comment refers to as the "particularity approach."[130] This approach promotes new private search rules specifically designed to accommodate the unique complexities of electronic devices.[131] Section A describes the particularity approach. Section B examines

---

[127] *Id.* at 838.

[128] *See id.* This Comment suggests that this reasoning was circular, as the court determined that the police were "substantially certain" of the contents because the private searchers were "substantially certain" of the contents. *Id.* However, other courts have applied the "substantially certain" test in the context of electronic devices and have reached decisions that are seemingly inconsistent with *Runyan* and *Rann*. *See, e.g.*, United States v. Crist, 627 F. Supp. 2d 575, 585–87 (M.D. Pa. 2008) (holding that the government search of a computer "exceeded the scope of the private search because the Government was not substantially certain the computer contained only contraband"); People v. Michael E., 178 Cal. Rptr. 3d 467, 475–77 (Cal. Ct. App. 2014) (holding that the police search exceeded the scope of the private search because the officers were not "substantially certain" of the contents of video files on a flash drive). Despite repeated citations to the *Runyan* decision throughout the *Crist* and *Michael E.* opinions, these applications of the "substantially certain" test imply that government officials can only ever be substantially certain of the contents of the particular videos, images, or other items actually viewed by the private searcher, rather than all the contents of a "container" opened by a private searcher, as suggested by *Runyan* and *Rann*. *See Crist*, 627 F. Supp. 2d at 586–87; *Michael E.*, 178 Cal. Rptr. 3d at 478–81.

[129] *Rann*, 689 F.3d at 837 (quoting *Runyan*, 275 F.3d at 463–64).

[130] *See, e.g.*, United States v. Sparks, 806 F.3d 1323, 1336 (11th Cir. 2015); United States v. Lichtenberger, 786 F.3d 478, 485–89 (6th Cir. 2015); United States v. Wicks, 73 M.J. 93, 100–01 (C.A.A.F. 2014).

[131] *See* Clancy, *supra* note 20, at 202–03 (referring to this approach as the "special approach" and stating that courts utilizing this approach suggest that electronic data searches require different rules and procedures

the Sixth Circuit's use of the particularity approach. Section C describes the Eleventh Circuit's employment of the particularity approach. Section D explores the Court of Appeals for the Armed Forces's application of the particularity approach.

A. Description of the Particularity Approach

The particularity approach stems from the reality that computers and other electronic devices are "fundamentally different from a writing, or a container of writings."[132] These fundamental differences include the immense storage capacity of electronic devices, the communicative function that permits electronic device users to connect via the Internet, and the private nature of data likely stored on electronic devices.[133] The particularity approach suggests that these fundamental differences create unique issues that traditional private search rules do not address.[134] Hence, the particularity approach proposes "unique procedures and detailed justifications" to address the issues that traditional private search rules neglect.[135]

The particularity approach developed independently in different jurisdictions, but the common thread among applications remains the agreement that government searches of electronic devices should be narrowly-tailored.[136] The most well-known applications of the particularity approach are the Sixth Circuit's 2015 decision in *United States v. Lichtenberger*,[137] the Eleventh Circuit's 2015 decision in *United States v. Sparks*,[138] and the U.S. Court of Appeals for the Armed Forces 2014 opinion in *United States v. Wicks*.[139] This Comment first addresses the circuit court opinions at the core of

---

than other searches). It is important to note that Professor Clancy rejects this "special approach." *Id.* at 196. However, his discussion of the approach is relevant to this Comment's analysis of the particularity approach.

132 *Id.* at 203 (quoting People v. Gall, 30 P.3d 145, 162 (Colo. 2001) (en banc) (Martinez, J., dissenting)).

133 *Id.*

134 *Id.*

135 *Id.* at 196.

136 *See id.* at 203 ("Moreover, Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers . . . ." (quoting *Gall*, 30 P.3d at 162)); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547–48 (2005) (referring to this approach as the "exposure-based approach" and stating that "government agents may view only the information viewed by the private actor unless they first obtain a warrant").

137 786 F.3d 478, 487 (6th Cir. 2015).

138 806 F.3d 1323, 1336 (11th Cir. 2015).

139 73 M.J. 93, 102 (C.A.A.F. 2014).

the circuit split and then discusses the first-in-time U.S. Court of Appeals for the Armed Forces decision.

B. The Sixth Circuit's Application of the Particularity Approach

The Sixth Circuit applied the particularity approach in *United States v. Lichtenberger*.[140] In *Lichtenberger*, a private searcher accessed the defendant's private, password-protected laptop.[141] She opened various folders on the laptop and discovered images of child pornography.[142] Then, she called the police to report her findings.[143] When an officer arrived, he instructed the private searcher to open the laptop and show him the images.[144] She opened the computer and clicked on "random thumbnail images to show him."[145] She later stated "that she could not recall if [the images she showed the police officer] were among the same photographs she had seen earlier . . . ."[146]

The defendant was indicted and later filed a motion to suppress the evidence that the officer obtained from his warrantless search.[147] In his motion, the defendant asserted that the private searcher was acting as an agent of the government when the officer instructed her to open the images she found.[148] The district court granted the defendant's motion to suppress on agency grounds, but the government appealed the case to the Sixth Circuit Court of Appeals.[149]

The Sixth Circuit Court distinguished its decision from that of the lower court by arguing that the relevant issue was scope rather than agency.[150] To that end, the court compared the scope of the initial private search to that of the subsequent government search using two criteria stemming from the traditional private search doctrine case *Jacobsen*: (1) "how much information the

---

[140] *See* 786 F.3d at 487 (stating that "searches of physical spaces and the items they contain differ in significant ways from searches of complex electronic devices under the Fourth Amendment").

[141] *Id.* at 480.

[142] *Id.* She later testified that she viewed about one hundred images during her private search. *Id.* at 481.

[143] *Id.* at 480.

[144] *Id.*

[145] *Id.*

[146] *Id.* at 488.

[147] *Id.* at 481.

[148] *Id.*

[149] *Id.*

[150] *Id.* at 485 ("Accordingly, the correct inquiry is whether [the police officer's] search remained within the scope of [the private searcher's] earlier one."). The court stated that the issue of agency should be addressed after "comparing the scope of the two searches." *Id.*

government stands to gain when it re-examines the evidence . . ."; and (2) whether the police officer had "virtual certainty" of what he would find during the subsequent government search.[151] While the court acknowledged that these factors have been at the core of private search analysis for decades and remain so in the context of electronic devices, it also stated that the unique characteristics of electronic devices and the privacy interests at stake alter the "virtual certainty" analysis, placing additional weight on preserving those privacy interests from warrantless government intrusion.[152] Thus, given the immense storage capacities of laptop computers, the court determined that "there [was] no virtual certainty that [the police officer's] review was limited to the photographs from [the private searcher's] earlier search . . . ."[153] Further, the court noted not only that the police officer could have viewed photos that the private searcher had not viewed, but also that the officer could have accessed other data that was potentially "private, legal, and unrelated to the allegations prompting the search."[154] The court stressed the Supreme Court's intent to prevent that very outcome.[155]

Given the potential for the government searcher to view data outside that which the private searcher viewed, the court held that the government search exceeded the scope of the private search and violated the defendant's Fourth Amendment rights.[156] The dispositive fact in reaching this holding was that the private searcher did not know whether the government search was limited to the particular images she viewed.[157] This holding suggests that subsequent government searches should be narrow and particularized to the material actually viewed during the private search, unlike the search at issue in the instant case.[158] In so doing, the Sixth Circuit set the stage for the circuit split and this Comment by emphasizing the fundamental differences between

---

151 *Id.* at 485–86 (citing United States v. Jacobsen, 466 U.S. 109, 119–20 (1984)).

152 *Id.* at 485–88 ("That the item in question is an electronic device does not change the fundamentals of this inquiry. But . . . the nature of the electronic device greatly increases the potential privacy interests at stake, adding weight to one side of the scale while the other remains the same. This shift manifests in *Jacobsen*'s 'virtual certainty' requirement." (citation omitted)).

153 *Id.* at 488 ("Considering the extent of information that can be stored on a laptop computer . . . the 'virtual certainty' threshold in *Jacobsen* requires more than was present here.").

154 *Id.* at 488–89.

155 *Id.* at 489.

156 *Id.* at 485.

157 *See id.* at 490.

158 *See id.* at 488–89 (suggesting that the subsequent government search must be limited to what, in particular, the private searcher viewed). This holding also suggests that the expectation of privacy in all the contents of the laptop was not frustrated by the private search, but rather it was frustrated only in the particular images the private searcher viewed. *See id.*

searches of traditional containers and searches of computers as well as the need for a narrow approach to accommodate these differences.[159]

C. The Eleventh Circuit's Application of the Particularity Approach

The Eleventh Circuit Court of Appeals deepened the circuit split when it applied the particularity approach in *United States v. Sparks*.[160] Like the Sixth Circuit's application in *Lichtenberger*, the Eleventh Circuit's application suggests a narrow, particularized concept of scope.[161]

The defendants in *Sparks* accidentally left a cell phone at a Walmart store, but a store employee discovered the misplaced phone.[162] After locating the phone, the employee noticed messages from the defendants requesting return of the phone and providing a contact number to arrange its return.[163] The employee contacted the defendants using the number provided and agreed to return the phone.[164] However, before meeting with the defendants, the employee decided to look at images stored on the cell phone so she could identify its true owner.[165] During her examination, the employee discovered "questionable" images of a young girl in the photo album.[166] The employee then showed the images to the private searcher.[167] They looked at thumbnail images of all the photographs in the photo album and two full-sized images.[168] The private searcher then took the phone to the Fort Myers Police Department.[169] At the Fort Myers Police Department, he met with several Community Service Aides, scrolled through all the thumbnails in the photo album, showed them several full-sized images, and played them a video.[170] Then, the Community Service Aides contacted a sergeant, who viewed the

---

159 *See id.* at 487 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [our prior cases]." (quoting Riley v. California, 134 S. Ct. 2473, 2485 (2014))).

160 *See* 806 F.3d 1323, 1334–36 (11th Cir. 2015); *see also* Orin Kerr, *11th 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/.

161 *See Sparks*, 806 F.3d at 1336.

162 *Id.* at 1330.

163 *Id.*

164 *Id.*

165 *Id.*

166 *Id.* at 1330–31.

167 *Id.*

168 *Id.* at 1331.

169 *Id.*

170 *Id.*

images in the photo album and two videos.[171] Notably, the private searcher had only watched one of these videos.[172]

The sergeant sent the phone to the police department for the city in which the Walmart was located, and the department assigned the case to an agent.[173] The agent applied for a warrant to search the phone and submitted a supporting affidavit from the sergeant regarding his search of the phone.[174] A judge granted the warrant, and the agent conducted a forensic examination of the phone.[175] Based on evidence from the forensic examination of the phone, the agent obtained a search warrant for the defendants' residence.[176]

The defendants moved to suppress the evidence obtained from both the warrants, but the district court denied the motions.[177] The defendants appealed the district court's decision based on three arguments: (1) the sergeant's search of the phone exceeded the scope of the private search, (2) the gap in time between the agent receiving the case and applying for the search warrants was an unreasonable interference with possessory interests, and (3) the search warrant should have been backed by more than just the sergeant's description of the images.[178] The court deepened the circuit split and applied the particularity approach in its analysis of the first prong of the appeal—whether the district court erred in concluding that the sergeant's warrantless search of the cell phone did not exceed the scope of the private search.[179]

First, the court addressed whether the sergeant's review of all the pictures in the photo album replicated or exceeded the scope of the private search.[180] The court ultimately agreed with the district court and held that the government search of the pictures merely replicated the scope of the private search.[181] The private searcher viewed thumbnail images of *every* picture in

---

171 *Id.* at 1331–32.
172 *Id.* at 1332.
173 *Id.*
174 *Id.* at 1332–33.
175 *Id.* at 1333.
176 *Id.*
177 *Id.* The district court denied the motions to suppress because they found that the sergeant's warrantless search of the phone did not exceed the scope of the private search. *Id.*
178 *Id.*
179 *Id.* at 1334–37.
180 *Id.* at 1335.
181 *Id.*

that photo album on several different occasions.[182] Further, "[the sergeant] specifically testified that he looked at only those images contained in a single photo album, and his description of the thumbnails of the photos contained in that album matched the contents of the album that [the private searcher] had viewed."[183] Thus, the court concluded that the sergeant's search of the pictures in that photo album was a permissible replication of the private searcher's review of all the thumbnails in that album.[184]

Next, the court considered whether the sergeant's warrantless search of the videos exceeded the scope of the private search.[185] On this, the court disagreed with the district court and found that the sergeant's review of the video the private searcher did not view exceeded the scope of the private search.[186] The court stressed the fact that the private searcher had only viewed one of the two videos that the sergeant viewed during his search.[187] The private searcher never viewed the second video, although it was located in the same photo album that the private searcher scrolled through on numerous occasions.[188] Thus, the court found that the sergeant exceeded the scope of the private search when he viewed the video that the private searcher did not view, and the private search of the cell phone frustrated the expectation of privacy in some of the contents of the phone, but not all.[189] However, the court found that there was no reversible error because the district court's conclusion, though incorrect, did not influence the warrant outcome.[190]

In brief, the Eleventh Circuit held that viewing the same material as the private searcher does not exceed the scope of the private search.[191] Therefore, the sergeant did not violate the defendants' Fourth Amendment rights when he

---

[182] *Id.* The private searcher first viewed the entirety of the photo album with his fiancé, the Walmart employee who found the phone. *Id.* Then, he viewed them again before handing the phone over to a Community Service Aide. *Id.* Finally, he viewed the images with two other Community Service Aides. *Id.*

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.* at 1336 ("But with respect to the second video, which [the private searcher] never watched, [the sergeant's] review exceeded—not replicated—the breadth of the private search.").

[188] *Id.* at 1335.

[189] *Id.* at 1336 ("While [the private searcher's] private search of the cell phone might have removed certain information from the Fourth Amendment's protections, it did not expose every part of the information contained in the cell phone.").

[190] *Id.* at 1336–37. This conclusion did not change the probable cause determination because the sergeant's affidavit in support of the warrant application did not reference the video that the private searcher did not view. *Id.*

[191] *Id.* at 1336.

viewed the full-sized versions of the thumbnail images the private searcher viewed.[192] However, the private search doctrine does not permit a government searcher to conduct a warrantless search of material that the private searcher did not actually view.[193] Thus, the Eleventh Circuit utilized a narrow, particularized concept of scope for private searches of electronic devices by holding that the private search doctrine only permits government review of the particular material viewed during the private search.[194] The Petition for Writ of Certiorari was denied on May 16, 2016.[195]

D. The Court of Appeals for the Armed Forces's Application of the Particularity Approach

The U.S. Court of Appeals for the Armed Forces applied the particularity approach in *United States v. Wicks*.[196] This application resulted in an even more specific concept of scope than the Sixth and Eleventh Circuits' applications.[197]

In *Wicks*, the private searcher stole the appellant's cell phone and saw text messages that she thought were "inappropriate" for the appellant's position as a military training instructor.[198] Several months later, the private searcher told the Security Forces Office of Investigations (SFOI) about the text messages.[199] To substantiate her claims, the private searcher gave a detective from the SFOI a cell phone, which she claimed did not belong to the appellant but that held information downloaded from the appellant's phone.[200] Once in SFOI possession, government agents searched the phone on three separate occasions without obtaining a warrant.[201] First, the SFOI detective randomly viewed

---

192 *Id.*

193 *Id.*

194 *Id.* at 1334–36.

195 United States v. Sparks, 136 S. Ct. 2009 (2016) (mem.). While the Petition mentioned the private search doctrine and the definition of the scope of a private search involving electronic devices, the two reasons provided for why certiorari should have been granted were facially unrelated to the scope issue: (1) the majority erred in holding that the phone was abandoned and the defendant lacked standing to challenge the delay in obtaining a warrant and that the majority erred in finding that the court lacked jurisdiction to consider the motion to suppress; and (2) the majority's holding that the defendant did abandon the phone was in conflict with other circuit's decisions. Petition for Writ of Certiorari, *Sparks*, 806 F.3d 1323 (No. 15-7733).

196 *See* 73 M.J. 93, 100–01 (C.A.A.F. 2014).

197 *See id.*; *see also supra* notes 140–95 and accompanying text.

198 *Id.* at 96.

199 *Id.*

200 *Id.* at 97.

201 *Id.*

some of the text messages on the phone.[202] Then, the detective gave the cell phone to the local sheriff's office and requested an analysis of the entire cell phone.[203] Finally, the SFOI sent the phone out to a third party for additional analysis.[204] The third party viewed over 45,000 text messages during its comprehensive analysis.[205]

In analyzing the searches, the Court of Appeals for the Armed Forces asked: (1) whether the appellant had a reasonable expectation of privacy in his cell phone, (2) whether the private searcher frustrated that expectation of privacy so as to permit the subsequent government searches, and (3) whether the government searches exceeded the scope of the private search.[206] First, the court determined that the appellant did have a reasonable expectation of privacy in the cell phone.[207] Second, the court concluded that the private searcher frustrated the expectation of privacy *in the text messages that she viewed*.[208] Therefore, the government could lawfully conduct a warrantless search of those same messages pursuant to the private search doctrine.[209] Third, the court determined that although the Government could have searched the text messages in which the expectation of privacy was frustrated, the subsequent government searches exceeded the scope of the private search.[210] The court held that the subsequent government searches exceeded the scope of the private search in "a material qualitative and quantitative manner" because the detective did not limit her search of the text messages to those the private searcher viewed; the Government did not regard the appellant's Fourth Amendment rights in turning the cell phone over to the sheriff's office or the third party; and the third-party search included over 45,000 text messages,

---

202 *Id.*

203 *Id.* (describing how the detective told the sheriff's office that it was a "consent search" but did not provide paperwork regarding the consent). The local sheriff's office discovered that the only information on the phone was the appellant's data, which was irregular for a phone that allegedly belonged to someone other than the appellant. *Id.* The private searcher eventually admitted that the cell phone actually belonged to the appellant. *Id.*

204 *Id.*

205 *Id.*

206 *Id.* at 98–101.

207 *Id.* at 99 (explaining that cell phones provide communication functions and data storage functions that necessitate Fourth Amendment protection).

208 *Id.* at 99–101 ("And although Appellant's expectation of privacy had been frustrated by [the private searcher] viewing a few text messages and the accompanying video, it was not eliminated altogether . . . .").

209 *Id.* at 100 ("As such, once a private party has conducted a search, any objectively reasonable expectation of privacy a person may have had in the material searched is frustrated with respect to a subsequent government search of the same material.").

210 *Id.* at 100–01.

including both existing and deleted messages.[211] Further, the court clearly articulated the particularity requirement when it stated, "[a]pplying [the private search doctrine] to modern computerized devices like cell phones, the scope of the private search can be measured by what the private actor *actually* viewed as opposed to what the private actor had access to view."[212]

In sum, the Court of Appeals for the Armed Forces's application of the particularity approach employs an extremely narrow concept of scope, protecting individuals against broad, expansive government searches.[213] The court also went on to dismiss the container approach by stating, "if one likens turning on a cell phone to opening a container, then everything within the cell phone would lose its privacy protections where the private party merely turned the phone on before turning it over to the government."[214]

IV. THE PARTICULARITY APPROACH IS SUPERIOR

The circuit split presented above represents a weighty debate between a broad, permissive scope on one hand and a narrow, particular scope on the other. This Comment argues that examination of the strengths and weaknesses of both approaches reveals the superior approach: the particularity approach. Section A assesses the container approach and determines that it disregards the fundamental differences between electronic devices and static containers. Section B discusses the particularity approach and determines that its strengths greatly outnumber its arguable weaknesses. Therefore, courts should adopt the particularity approach, and, in the event this issue reaches the Supreme Court, the Court should also apply the particularity approach.

A. The Container Approach Ignores the Unique Characteristics of Electronic Devices

While it has some arguable benefits, the container approach's many shortcomings call its merits into question. This section discusses the potential benefits of the container approach and then addresses its many downfalls.

---

211 *Id.* at 101.
212 *Id.* at 100.
213 *See id.*
214 *Id.*

1. Arguable Positives of the Container Approach

The container approach has several benefits that contribute to the Fifth and Seventh Circuits' decisions to utilize the approach. First, it benefits government searchers by removing the pressure to keep within the literal scope of a private search. Second, it reduces the monetary and material burden on government agencies overseeing the searches. Third, it eases the burden on private searchers. Fourth, it simplifies the task for courts charged with determining scope.

First, the container approach removes the strain on government officials to stay within the literal scope of a private search. The Fifth Circuit in *Runyan* stated that a government official can search all the contents of a disk if the private searcher opened and examined at least some of its contents.[215] Thus, under the container approach, government officials have broad authority to search devices more thoroughly and view more files without fear of violating the owners' Fourth Amendment rights.[216] Therefore, they are free to discover incriminating evidence without the worry that they will exceed the scope of the private search and that a court will exclude the evidence pursuant to the exclusionary rule.[217] It follows that government officials in jurisdictions that utilize the container approach may be able to admit additional evidence of criminality and prosecute more criminals than those in jurisdictions that use the narrower particularity approach.

In addition, the container approach removes the strain on government officials by providing a degree of flexibility for government searchers. Specifically, if a government agent opens a file that the private searcher did not open, he could justify the expansion of the scope under the container approach because it permits searches of files not opened by the private searcher.[218] So, the government agent could argue that he did not exceed the scope of the

---

[215] United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) ("[T]he police do not exceed the private search when they examine more items within a closed container than did the private searchers.").

[216] *See id.* at 465 (explaining that the opposite holding, a finding that the police exceed the scope of the private search by examining more items in a container than the private searcher, would result in "fear of coming across important evidence that the private searchers did not happen to see and that would then be subject to suppression").

[217] *See* Matthew Allan Josephson, *To Exclude or Not Exclude: The Future of the Exclusionary Rules After* Herring v. United States, 43 CREIGHTON L. REV. 175, 179 (2009). But, deterrence is an essential policy component of the exclusionary rule. *See* United States v. Calandra, 414 U.S. 338, 347–48 (1974) ("[T]he rule's prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures . . . .").

[218] *See* People v. Michael E. 178 Cal. Rptr. 3d 467, 475, 479 (Cal. Ct. App. 2014).

private search when he viewed something outside the literal scope.[219] Thus, the container approach gives government searchers more flexibility and freedom than the particularity approach to discover potentially incriminating evidence without obtaining a warrant.

Second, the container approach reduces the fiscal burden on government agencies. The container approach keeps officials from having to expend time, money, and effort to obtain a warrant in order to view additional files on the same device.[220] Instead, they can rely on *Runyan* to view additional files without exceeding the scope of the private search, requiring a warrant.[221] The ability to search additional files without having to obtain a warrant could prove helpful in cases such as *Runyan*, where files that the private searchers did not view contained images of child pornography.[222] In such cases, the government searchers are free to discover these additional images and pursue legal action based on the additional evidence obtained without a warrant.

Third, the container approach reduces the burden on private searchers to view all the evidence on a device before turning it over to government officials. The burden on private searchers is lower pursuant to the container approach because a private searcher conducting a search in a jurisdiction that applies the container approach does not have to search every file on a device before handing it over to government officials.[223] The private searcher could theoretically view only one file. Yet, that limited private search would be sufficient to grant police the authority to search the entire disk or device pursuant to *Runyan*, which suggests that the expectation of privacy in *all* the contents of a disk is frustrated when a private searcher merely opens the disk.[224]

Fourth, the container approach benefits courts because they can rely on existing private search doctrine rules rather than having to develop specialized rules. Advocates of a container analogy suggest that electronic devices store physical evidence, just as traditional containers; so, there is no need for special

---

219 *See id.*

220 *See Runyan*, 275 F.3d at 465 (explaining that limiting the scope of government searches to only the materials private searchers viewed would result in the "waste [of] valuable time and resources obtaining warrants").

221 *See id.* at 464.

222 *See id.* at 454.

223 *See id.* at 464.

224 *See id.*

Fourth Amendment standards.[225] In this same vein, the container approach proposes that the established Fourth Amendment rules for traditional containers are also applicable to computers.[226] These arguments allow courts to opt to apply existing case law rather than to develop new, specialized legal standards.[227]

2. Numerous Shortcomings of the Container Approach

Despite the above benefits, the container approach has numerous and significant weaknesses. First, the container approach neglects the unique privacy concerns associated with electronic devices. Second, it fails to clearly answer the question of scope. Third, the container approach is contrary to the Fourth Amendment warrant requirement and the policy justifications for the warrant preference rule. Fourth, it ignores the fundamental differences between electronic devices and traditional containers.

First, the container approach yields troublesome privacy concerns that outweigh the government interests at stake. Courts frequently identify a careful balance between government interests and privacy concerns in the context of Fourth Amendment issues.[228] The unique privacy issues and the unparalleled storage potential associated with electronic devices alter this careful balance.[229] However, the container approach fails to accommodate that shift—*Runyan* illustrates this failure perfectly. *Runyan* asserts that if a private searcher merely opens a disk, then all of the contents of that disk are subject to a subsequent government search.[230] The over-breadth of this proposition has significant

---

225 *See, e.g.*, Clancy, *supra* note 20, at 196 ("As with all containers, [computers] have the ability to hold physical evidence, including such items as wires, microchips, and hard drives. . . . Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers.").

226 *See id.*

227 *See id.* (arguing that the approach that views computers and containers as equivalents for Fourth Amendment purposes is superior to the "special approach," which "require[es] unique procedures and detailed justifications").

228 *See, e.g.*, United States v. Lichtenberger, 786 F.3d 478, 487 (6th Cir. 2015); United States v. Erickson, 991 F.2d 529, 531 (9th Cir. 1993); United States v. Epperson, 454 F.2d 769, 771 (4th Cir. 1972) ("The reasonableness of any search must be determined by balancing the governmental interest in searching against the invasion of privacy which the search entails."). For a recommendation that courts should implement a balancing test specifically to accommodate searches of cell phones incident to arrest, see Drew Liming, *Calling for a Standard: Why Courts Should Apply a New Balancing Test in Cell Phone Searches Incident to Arrest*, 51 AM. CRIM. L. REV. 715, 729–30 (2014).

229 *See Lichtenberger*, 786 F.3d at 487–88.

230 *See Runyan*, 275 F.3d at 464–65 (explaining that police do not need to get a warrant to search each item in a container that the private searcher opened and partially searched).

privacy implications because it ensures that police have access to anything stored on a device, including potentially private information.[231] Not only does the container approach result in government officials potentially stumbling upon sensitive information, but government searches also have the potential to reach vast quantities of this private information due to the colossal storage capacities of electronic devices. Hence, the container approach encourages intrusive government searches and broad invasions of privacy, in direct conflict with the spirit of the Fourth Amendment.

Second, the container approach fails to consistently delineate the boundaries of the "container" at issue. The container approach does not definitively answer whether the container is the entire device or a smaller subdivision within the device. Even courts that agree on the application of the container approach do not agree on what the container actually is.[232] *Runyan* suggests that the relevant unit is the disk or device as a whole.[233] However, other Fourth Amendment cases, including the district court case *United States v. Barth*[234] suggest that the relevant unit in a container analogy is the file. Such cases assert that each file is a "sub-container" inside a larger container—the folder.[235] Still others argue that the container is the folder.[236] Disagreement over the bounds of the container inevitably fosters inconsistent applications of the container approach. This inconsistency creates a challenge in predicting how courts will apply the container approach across jurisdictions.

---

231 *See* United States v. Wicks, 73 M.J. 93, 100 (C.A.A.F. 2014) (stating that the container analogy, like in *Runyan*, would result in "everything within [a] cell phone [losing] its privacy protections where the private party merely turned the phone on before turning it over to the government"); *Lichtenberger*, 786 F.3d at 488–89 (stating that the government official easily could have stumbled upon information "that was private, legal, and unrelated to the allegations" on the laptop, contrary to Fourth Amendment intent).

232 *See* Holley, *supra* note 114, at 691–96.

233 *Runyan*, 275 F.3d at 464–65; Holley, *supra* note 114, at 694–95.

234 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998) (explaining that the private searcher viewed several files and the police exceeded the scope of the private search when they viewed all the files on the hard drive); Holley, *supra* note 114, at 691–92.

235 *See Carey*, 172 F.3d at 1275–76; *Barth*, 26 F. Supp. 2d at 937; Holley, *supra* note 114, at 691–92; *see also* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 119 (2011) (calling this approach the "subcontainer perspective" that "conceptually divides a single hard drive, cell phone, or other storage medium into many subcontainers, each subcontainer requiring justification for its examination").

236 *See, e.g.*, People v. Emerson, 766 N.Y.S.2d 482, 488 (N.Y. Sup. Ct. 2003) (stating that the government searchers did not exceed the scope of the private search when they viewed additional images in the same folders that the private searcher viewed); *see also* Holley, *supra* note 114, at 692–94 (explaining that *Emerson* "seems to constrain law enforcement to searches conducted within the same folders, but not the same files, as the private search").

Third, the container approach is at odds with the warrant preference rule and its policy justifications. The Supreme Court has long recognized the warrant preference rule in Fourth Amendment cases.[237] While the Court has established numerous exceptions to the warrant preference rule, including the private search doctrine, it maintains, "[t]he exceptions cannot be enthroned into the rule."[238] Thus, even searches permitted under an exception to the warrant preference rule must be "confine[d] . . . to their appropriate scope"[239] and cannot be used to justify broad, intrusive warrantless searches.[240] The container approach is not "confine[d] . . . to [its] appropriate scope"[241] because it does not limit subsequent government searches to the particular scope of the private search. Rather, it permits government searchers to conduct broad, intrusive warrantless searches—including searches of material that the private searcher did not actually view—that the Fourth Amendment, the warrant preference rule, and the Supreme Court all seek to prevent.

In addition to its conflict with the warrant preference rule and the goals of the Fourth Amendment, the container approach also ignores the policy justifications behind the warrant requirement. The Fourth Amendment Framers included the warrant requirement because, in the words of the Supreme Court, "[t]he right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals."[242] Further, the warrant requirement places the discretion in the hands of neutral magistrates, guarding against the potentially flawed judgment of "well-intentioned, but mistakenly over-zealous executive officers."[243] The container approach ignores these policy justifications by placing the discretion in the hands of the government searchers and permitting them to exceed the literal scope of the private search without obtaining a warrant authorized by a neutral

---

237 *See* Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971).

238 *Id.* (quoting United States v. Rabinowitz, 339 U.S. 56, 80 (1950) (Frankfurter, J., dissenting)).

239 *Id.*

240 *Cf. Rabinowitz*, 339 U.S. at 79 (Frankfurter, J., dissenting) ("But to assume that this exception of a search incidental to arrest permits a free-handed search without warrant is to subvert the purpose of the Fourth Amendment . . . .").

241 *Coolidge*, 403 U.S. at 481.

242 McDonald v. United States, 335 U.S. 451, 455–56 (1948); *see also* Johnson v. United States, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.").

243 Gouled v. United States, 255 U.S. 298, 304 (1921); *see also McDonald*, 335 U.S. at 456 ("Power is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the Constitution requires a magistrate . . . .").

magistrate, just as in *Runyan*.[244] Thus, the container approach is at odds with the warrant requirement and the justifications of the warrant requirement.

Fourth, electronic devices are fundamentally different from traditional containers, making an analogy necessarily flawed.[245] These fundamental differences include storage capacities, privacy implications, and intrusiveness of the searches.[246]

Most significantly, modern electronic devices have tremendous storage capabilities that traditional containers lack.[247] Computers can store over eighty million pages of text, with that number constantly multiplying.[248] Professor Orin Kerr explains that houses, like electronic devices, can store many different types of evidence, but the quantity of information that can be stored in a home is severely restricted in comparison to the quantity of data that can be stored on an electronic device.[249] Professor Kerr's argument[250] extends to traditional containers: the storage capacity of a standard container is also limited to the physical size of that container. Conversely, "the storage capability of an electronic device is not limited by its physical size as a container is."[251] Rather, the quantity of information that can be stored on an electronic device is prodigious, particularly when taking into account the advancement of cloud computing.[252] Thus, government officials have access to considerably more information when they search an electronic device pursuant

---

244 *See supra* notes 101–25 and accompany text.

245 *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("Treating a cell phone as a container . . . is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen." (citation omitted)); *see also* Holley, *supra* note 114, at 682 ("The complex nature of computer storage makes application of [the container analogy] in the digital setting problematic.").

246 *See supra* text accompanying notes 8–18.

247 *See* United States v. Wurie, 728 F.3d 1, 9 (1st Cir. 2013) ("In short, individuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers that the government has invoked."); *see also* United States v. Mayo, No. 2:13-CR-48, 2013 WL 5945802, at *7 (D. Vt. Nov. 6, 2013).

248 *See* Holley, *supra* note 114, at 682 (invoking Moore's Law by stating that a computer in 2010 could store the equivalent of about eighty million pages of text, with that number duplicating about every two years).

249 Kerr, *supra* note 136, at 541–42.

250 *See id*. (explaining that the storage capacity of a house is limited by its square footage).

251 Shlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1169 (D. Or. 2012).

252 *See* Gordon K. Eng, *The Mobile Office Continues to Evolve*, 36 L.A. LAW., Sept. 2013, at 38, 39 (stating that Box, one of the leading cloud computing providers, offers "a promotion for 50 gigabytes of free storage"); William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199 (2010) (defining cloud computing as "the ability to run applications and store data on a service provider's computers over the Internet, rather than on a person's desktop computer"); Mark Wilson, Comment, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U. L. REV. 261, 262 (2013).

to the container approach compared to when they search a traditional container.[253] The container approach does not account for this storage disparity.[254]

The heightened privacy concerns associated with searches of electronic devices also present a fundamental difference that strains the application of the container approach.[255] Some suggest that electronic devices inherently merit additional Fourth Amendment protection.[256] Pursuant to this argument, the container approach does not provide sufficient protection, as it affords electronic devices exactly the same protection as traditional containers.[257] The container approach also neglects the privacy concerns relating to the types of information stored on electronic devices.[258] Electronic device users regularly store highly sensitive information on their devices, including medical and financial information.[259] Many also use e-mails, text messages, and other types of electronic messages to share personal, potentially embarrassing, information.[260] As Josh Goldfoot notes, people have always shared personal information with others, but there were never transcripts of these conversations.[261] However, text messages and e-mails now provide a physical

---

253 *See* Michael V. Hinckley, Comment, *An Unreasonable Expectation? Warrantless Searches of Cell Phones*, 2013 BYU L. REV. 1363, 1380–81.

254 United States v. Mayo, No. 2:13-CR-48, 2013 WL 5945802, at *7 (D. Vt. Nov. 6, 2013) ("The container analogy [in the context of searches incident to arrest] fundamentally fails to address the magnitude of modern cell phone storage capacity.").

255 *See* United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012); *see also* United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011); United States v. Payton, 573 F.3d 859, 861–62 (9th Cir. 2009).

256 *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009) (suggesting that electronic devices may be entitled to "preferred status," given their massive storage capacities); Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 SANTA CLARA L. REV. 183, 223 (2010) (concluding that cell phones "warrant heightened protection because of their capability for storing very large amounts of private data"). *But see* Goldfoot, *supra* note 235, at 164–65 (arguing that computers are not entitled to greater privacy protection on account of their storage capabilities because "Fourth Amendment protections do not shrink and expand with the size of the premises or container").

257 The container approach analogizes containers to electronic devices and applies the same standards to both, thereby affording them the same level of protection. *See* Clancy, *supra* note 20, at 240 (explaining that computers should be treated as filing cabinets for purposes of private search analysis and "rules regulating containers in the bricks and mortar world have equal applicability to computer searches").

258 United States v. Saboonchi, 990 F. Supp. 2d 536, 553 (D. Md. 2014) (citing United States v. Cotterman, 709 F.3d 952, 964–65, 968 (9th Cir. 2013)).

259 *See* United States v. Arnold, 454 F. Supp. 2d 999, 1003–04 (C.D. Cal. 2006), *overruled by* United States v. Arnold, 523 F.3d 941 (9th Cir. 2008).

260 *See* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) ("Individuals can . . . record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.").

261 Goldfoot, *supra* note 235, at 165–66.

record of conversations.[262] These types of records and transcripts are unique to electronic devices.[263] In sum, the highly personal types of data stored on other electronic devices are distinct from those stored in traditional containers, making the analogy at the core of the container approach even more tenuous.

Further, a search of an electronic device is likely to seem inherently more intrusive than a search of a traditional container.[264] "[T]he information contained in a laptop and in electronic storage devices renders a search of their contents substantially more intrusive than a search of the contents of a lunchbox or other tangible object."[265] As discussed above, people are increasingly keeping copies of confidential records exclusively on their electronic devices, which "implicate[s] dignity and privacy interests" due to the "sanctity of private thoughts memorialized on a data storage device" through these confidential records.[266] These "dignity and privacy interests" make searches of confidential electronic records feel more intrusive than searches of traditional containers.[267] By permitting broad, excessive searches of this private information, the container approach neglects the privacy concerns implicit in the private character of information stored on electronic devices.

All told, the container approach has numerous inadequacies, particularly privacy implications that outweigh the government interests at stake, undeveloped scope solution, conflict with the warrant requirement and its justifications, and nonchalance towards the fundamental differences between electronic devices and traditional containers.

B. The Particularity Approach Properly Considers the Practical Realities of Twenty-First Century Technology

This Comment suggests that the strengths of the particularity approach outweigh any argued weaknesses, and positions it as the best approach for determining the scope. This section (1) assesses the many strengths of the particularity approach, and (2) identifies and refutes two arguable weaknesses.

---

262 *Id.* ("Computers' growing utility may well cause individuals to structure more of their private lives around computer use, thus creating more physical evidence of what they do from hour to hour.").

263 *See id.*

264 *See* United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012); *Park*, 2007 WL 1521573, at *8; *Arnold*, 454 F. Supp. 2d at 1003–04.

265 *Arnold*, 454 F. Supp. 2d at 1003.

266 *Id.*

267 *Id.* at 1003–04.

1. Abundant Strengths of the Particularity Approach

This Comment argues that the particularity approach is the superior approach in the circuit split because it adapts Fourth Amendment law to the unique characteristics of electronic devices and avoids many of the shortcomings presented by the container approach. First, the particularity approach accommodates the unique characteristics of electronic devices rather than disregarding them. Second, the particularity approach takes into account the privacy concerns raised by electronic devices. Third, the particularity approach clearly defines the scope as opposed to leaving the issue open to court interpretation. Fourth, the particularity approach is directly comparable to the Supreme Court's influential decisions in *Walter*[268] and *Riley*.[269] Fifth, the particularity approach is consistent with the Framers' intent and the text of the Fourth Amendment. Finally, the particularity approach balances the often-competing interests of police efficiency and warrant preference.

First, the particularity approach avoids the inadequacies of the container approach by accommodating the unique characteristics of modern electronic devices as opposed to trying to fit them into an existing mold.[270] The fundamental differences between electronic devices and traditional containers are so numerous that the Supreme Court declared, comparing searches of the two categories for Fourth Amendment purposes "is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[271] The particularity approach embraces, rather than ignores, these stark differences and views them as the impetus for a specialized approach.[272] For example, the Court of Appeals for the Armed Forces in *Wicks* highlighted the characteristics of electronic devices that set them apart from traditional containers and necessitate the particularity approach.[273] Namely, the court focused on electronic devices' unique ability to link with other private systems, such as

---

268 *See supra* notes 55–70 and accompanying text.

269 *See supra* notes 1–19 and accompanying text.

270 *See* United States v. Wicks, 73 M.J. 93, 102 (C.A.A.F. 2014) (stating that the container analogies do not consider the unique challenges associated with modern electronic devices); *see also In re* Cellular Tel.'s, No. 14-MJ-8017-DJW, 2014 WL 7793690, at *4 (D. Kan. Dec. 30, 2014) ("The danger, of course, is that courts will rely on inapt analogical reasoning and outdated precedent to reach their decisions. To avoid this potential pitfall, courts must be aware of the danger and strive to avoid it by resisting the temptation to rationalize the application of ill-fitting precedent to circumstances [involving electronic devices].").

271 Riley v. California, 134 S. Ct. 2473, 2488 (2014).

272 *See Wicks*, 73 M.J. at 102–03.

273 *See id.* at 102. These differences include the immense storage capacities of electronic devices, the different organizational techniques utilized by electronic devices, the various protections that electronic device users can employ to protect their data, and the complex functions that electronic devices provide. *See id.*

bank accounts and security systems.[274] A broad search of an electronic device, such as those permitted by the container approach, could provide government officials access to all of these connected systems, potentially including private bank data and home security information.[275] On the other hand, a search of a traditional container would not include access to a vast, interconnected web of information.[276] The particularity approach accounts for these differences by narrowing the scope of the subsequent government search and preventing government officials from gaining access to the linked, private systems.[277]

Second, the particularity approach circumvents the deficiencies of the container approach by balancing the increased privacy concerns associated with electronic devices against government interests. Electronic devices are capable of storing greater quantities and varieties of data than traditional containers.[278] Additionally, there is a positive correlation between that storage capacity and the probability that electronic devices hold highly personal information.[279] The substantial likelihood that electronic devices hold personal information makes any search of an electronic device seem more invasive than that of a traditional container.[280] For instance, an individual would likely feel that his privacy was invaded more following a search of his smart phone, including any applications, communications, and financial information on that phone, than he would after a search of a shoebox full of his receipts. This simplified example illustrates the invasive nature of electronic device searches and alludes to the greater privacy interests at stake.[281] In keeping with the particularity approach, the Sixth Circuit argues that these increased privacy interests alter the careful balance of privacy and government interests, tipping the scale in favor of preserving privacy interests.[282] The particularity approach accommodates this shift and places increased emphasis on privacy concerns by narrowly and literally interpreting the scope.[283] In so doing, the particularity

---

274 *Id.*

275 *See id.*

276 *See id.*

277 *See id.* at 102–03.

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

279 *See id.*

280 *See* United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012) ("The potential invasion of privacy in a search of a cell phone is greater than in a search of a 'container' in a conventional sense . . . .").

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

282 *See id.*

283 *See id.* at 488–89 (finding that the reason that the government search exceeded the scope of the private search was that it was not limited to what the private searcher viewed and could have extended to personal, but legal, data stored on the computer).

approach ensures that subsequent government searches do not infringe on "unfrustrated" expectations of privacy by extending to material that was not actually searched during the private search.

Third, the particularity approach answers the scope question that the container approach neglects to fully address. The container approach analogizes electronic devices to containers, but does not clearly delineate the bounds of the container.[284] Further, the Fifth Circuit's application of the container approach draws a fuzzy, arbitrary line.[285] On the other hand, the particularity approach clearly answers the question of scope: the scope is limited to what exactly the private searcher viewed.[286] It is clear that, regardless of the type of device, the scope is limited to the particular material viewed during the private search. Thus, the particularity approach ensures harmonious application across jurisdictions.

Fourth, the particularity approach is superior because it is consistent with the private search precedent in *Walter*[287] and *Riley*.[288]

The Supreme Court in *Walter* utilized a narrow scope and held that projecting the film, as opposed to attempting to view it by holding it up to light, exceeded the scope of the private search.[289] Similarly, the Sixth Circuit, the Eleventh Circuit, and the Court of Appeals for the Armed Forces utilized a narrow scope in their applications of the particularity approach.[290] In addition, the Court in *Walter* stated, "the private party had not *actually* viewed the films."[291] This statement is directly comparable to a statement at the core of the particularity approach application in *Wicks*—"the scope of the private search can be measured by what the private actor *actually* viewed as opposed to what the actor had access to view."[292] Both of these statements stress what was *actually viewed* during the private search, and determinations of what the private searchers actually viewed directly informed the holdings in both cases. In *Walter*, the statement precedes the holding that projecting the film exceeded

---

284 *See supra* notes 232–36 and accompanying text.

285 *See* United States v. Runyan, 275 F.3d 449, 463–65 (5th Cir. 2001). The court implies that each disk is a separate container, but does not explain the implications for other types of technology. *See id.*

286 *See* United States v. Wicks, 73 M.J. 93, 100 (C.A.A.F. 2014).

287 *See supra* notes 55–70 and accompanying text.

288 *See supra* notes 1–19 and accompanying text.

289 447 U.S. 649, 657 (1980).

290 *See supra* notes 140–214 and accompanying text.

291 *Walter*, 447 U.S. at 657 (emphasis added).

292 United States v. Wicks, 73 M.J. 93, 100 (C.A.A.F. 2014).

the scope of the private search.[293] In *Wicks*, the statement comes before a discussion of how the various subsequent searches exceeded the scope of the private search.[294] *Lichtenberger* and *Sparks* also stress the importance of what the private searcher viewed in reaching their holdings.[295] Therefore, the particularity approach yields analyses and holdings consistent with *Walter*.

Moreover, the particularity approach is consistent with *Riley*, where the Court similarly determined that rules for searches of traditional objects do not have "much force with respect to digital content on cell phones."[296] Due to the unique characteristics of cell phones, the Court in *Riley* determined "that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[297] Although there is an established warrant exception for searches incident to arrest,[298] the Court required a warrant to search a cell phone incident to arrest because cell phones are inherently different from objects traditionally seized incident to arrest.[299] Similarly, the particularity approach requires police to obtain a warrant before searching outside the literal scope of the private search[300] to preserve the unique privacy interests associated with searches of electronic devices. Thus, the particularity approach is consistent with the Supreme Court's movement toward specialized Fourth Amendment rules for electronic devices.

---

293 *Walter*, 447 U.S. at 657 ("[T]he private party had not actually viewed the films. Prior to the Government screening, one could only draw inferences about what was on the films. The projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search. That separate search was not supported by any exigency, or by a warrant . . . ." (footnote omitted)).

294 *Wicks*, 73 M.J. at 100–01 (stating that the scope of the private search was limited to what the private searcher "actually viewed," evaluating the various subsequent searches and concluding that "in both a material qualitative and quantitative manner, the Government exceeded the scope of the initial private search").

295 *See* United States v. Sparks, 806 F.3d 1323, 1335 (11th Cir. 2015) ("To the extent that [the sergeant] viewed the second video, . . . which [the private searcher] did not view, we agree . . . that [the sergeant] exceeded the scope of [the] private search."); United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) ("[The private searcher] admitted during testimony that she could not recall if [the photos she showed the police officer] were among the same photographs she had seen earlier . . . .").

296 *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014). The Court also explicitly rejected a container analysis because of the ability of cell phones to access a network of information. *Id.* at 2491 ("Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen." (citation omitted)).

297 *Id.* at 2493.

298 *Id.* at 2482.

299 *Id.* at 2493–95.

300 *See* United States v. Wicks, 73 M.J. 93, 100–01 (C.A.A.F. 2014).

Fifth, the particularity approach is superior because it is consistent with the Framers' intent and the language of the Fourth Amendment.[301] The Framers' primary goal in drafting the Fourth Amendment was to outlaw "general warrants," which "were unparticularized as to the place or things to be searched for,"[302] and "writs of assistance."[303] The Framers intended to preclude such broad grants of authority to government officials and to protect individuals from intrusive government action.[304] In keeping with the Framers' intent to prohibit broad, general searches, the particularity approach narrows the scope of the government search and limits it to specific material that the private searcher already viewed.[305] The particularity approach is also consistent with the text of the Fourth Amendment.[306] This Comment agrees with the *Walter* decision, which stated, "[i]f a properly authorized official search is limited by the particular terms of its authorization, at least the same kind of strict limitation must be applied to any official use of a private party's invasion of another person's privacy."[307] The particularity approach implements these limits by restricting the scope to the specific material that the private searcher viewed.[308] In sum, the particularity approach is consistent with the goals and language of the Fourth Amendment.

Finally, the particularity approach successfully balances the often-competing goals of police efficiency and warrant preference.[309] Police efficiency is a common consideration in Fourth Amendment law, and the Court has previously expressed the need for uniform rules that police officers can

---

301 *See supra* notes 34–37, 42–50 and accompanying text.

302 Thomas Y. Davies, *Can You Handle the Truth? The Framers Preserved Common-Law Criminal Arrest and Search Rules in "Due Process of Law"—"Fourth Amendment Reasonableness" is Only a Modern, Destructive, Judicial Myth*, 43 TEX. TECH L. REV. 51, 55 (2010).

303 Fabio Arcila, Jr., *In the Trenches: Searches and the Misunderstood Common-Law History of Suspicion and Probable Cause*, 10 U. PA. J. CONST. L. 1, 10 (2007); Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 980–84.

304 *See* Robert J. McWhirter, *Molasses and the Sticky Origins of the 4th Amendment*, 43 ARIZ. ATT'Y, June 2007, at 16, 32 ("[M]en like Adams and Madison broadly wanted to protect the 'right to be secure' from government intrusion.").

305 *See* United States v. Sparks, 806 F.3d 1323, 1336 (11th Cir. 2015); United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015); United States v. Wicks, 73 M.J. 93, 100 (C.A.A.F. 2014).

306 *See supra* note 30 and accompanying text.

307 Walter v. United States, 447 U.S. 649, 657 (1980).

308 *See Sparks*, 806 F.3d at 1336; *Lichtenberger*, 786 F.3d at 488–89; *Wicks*, 73 M.J. at 100–01.

309 *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 393 (1978) ("[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment.").

follow in the field.[310] The particularity approach provides one such "single, familiar standard"[311] because it limits subsequent government searches to the material actually viewed during the private search.[312] Therefore, the police have a clear, standard rule for all subsequent government searches, and there is relatively scarce ambiguity over what constitutes the bounds of the scope. Further, the particularity approach is consistent with the warrant requirement and warrant preference because it limits the discretion given to police by requiring them to search only within the literal scope of the private search, consistent with the Court's assessment of the warrant requirement.[313] Therefore, the particularity approach successfully balances the interests in police efficiency and warrant preference.

2. Argued Limitation of the Particularity Approach and Its Refutation

This Comment argues that the many strengths of the particularity approach outweigh the weaknesses. While the strengths of the particularity approach are significant and numerous, the weaknesses of the particularity approach are severely limited. In fact, the primary critiques are that the particularity approach is unnecessary[314] and that it may increase the burden on government officials.

In a dissenting opinion, Justice Stevens argued that a rule designed to accommodate "future technological developments" in a different area of Fourth Amendment doctrine was "unnecessary, unwise, and inconsistent with the Fourth Amendment."[315] Justice Stevens maintained that existing Fourth Amendment jurisprudence is sufficient, even in the context of electronic devices.[316] Others argue that the particularity approach is unwarranted because Fourth Amendment doctrine does not provide different rules for other types of containers like diaries and books.[317] They maintain that the lack of special

---

310 *See, e.g.*, Dunaway v. New York, 442 U.S. 200, 213–14 (1979) ("A single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront.").

311 *Id.* at 213.

312 *See Wicks*, 73 M.J. at 100.

313 *See id.*; *see also* McDonald v. United States, 335 U.S. 451, 455–56 (1948); Gouled v. United States, 255 U.S. 298, 304 (1921).

314 *See* Kyllo v. United States, 533 U.S. 27, 41–42 (2001) (Stevens, J., dissenting); *see also* Clancy, *supra* note 20, at 217–18 (arguing "that the Supreme Court would—and should—reject a special rule for electronic evidence containers").

315 *Kyllo*, 533 U.S. at 41 (Stevens, J., dissenting).

316 *Id.* at 41–42.

317 *See, e.g.*, Clancy, *supra* note 20, at 217–18.

rules for these types of containers indicates that different rules for different objects are unnecessary across the board.[318] Such rules may not have been appropriate in the past, but the advancement of technology has changed the legal landscape.[319] Many other areas of law have adapted to that change in the legal landscape precipitated by modern technology.[320] The private search doctrine should not be the exception to this evolution.[321]

Some critics of the particularity approach may also argue that it increases the burden on government searchers to stay within the narrow scope of the private search. However, the Supreme Court has previously dismissed similar arguments regarding police efficiency.[322]

In sum, this Comment suggests that the particularity approach is the best approach for determining the scope of a private search. The particularity approach accounts for the fundamental differences between electronic devices and other containers, balances the increased privacy concerns against the government interests at stake, answers the questions left open by the container

---

318 *See, e.g.*, *id.* ("[C]ontrary to Supreme Court precedent and sound reasoning, filing cabinets, diaries, books, floppy drives, hard drives, paper bags, and other storage devices would all require different rules."). Conversely, this Comment argues that traditional containers, such as filing cabinets and diaries, possess many of the same, static characteristics and merit similar rules; however, electronic devices are fundamentally and significantly different and require rules that accommodate these fundamental differences.

319 *See Kyllo*, 533 U.S. at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."); *see also* George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1452 (2005) ("[T]he Framers 'could hardly have been expected to foresee the current state of affairs.'" (quoting Yale Kamisar, *Does (Did) (Should) the Exclusionary Rule Rest on a "Principled Basis" Rather than an "Empirical Proposition"?*, 16 CREIGHTON L. REV. 565, 571 (1982–1983))).

320 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that there was a "search" when the government placed a tracking device on a vehicle and tracked its activity); United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (explaining that the "reasonableness determination must account for differences" between electronic devices and other types of property, like a gas tank or the bed of a pickup truck in the context of a border search); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (explaining that there was a reasonable expectation of privacy in e-mails stored through an Internet service provider and that the government's warrantless search of the e-mails violated the Fourth Amendment); State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (rejecting the container analogy for cell phone searches incident to arrest and stating that "because an individual has a privacy interest in the contents of a cell phone that goes beyond the privacy interest in an address book or pager, an officer may not conduct a search of a cell phone's contents incident to a lawful arrest without first obtaining a warrant").

321 *See* State v. Subdiaz-Osorio, 849 N.W.2d 748, 760 (Wis. 2014) ("Electronic devices afford us great convenience and efficiency, but unless our law keeps pace with our technology, we will pay for the benefit of our gadgets in the currency of privacy.").

322 *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 393 (1978) ("The investigation of crime would always be simplified if warrants were unnecessary. But the Fourth Amendment . . . may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law.").

approach, is consistent with Supreme Court precedent as well as the text and intent of the Fourth Amendment, and balances the interests in police efficiency and warrant preference. Further, the particularity approach has minimal downsides—the main oppositions being it is not completely necessary and it increases the burden on government searchers.[323] Given its many strengths, courts should adopt the particularity approach for determining the scope of private searches involving electronic devices. If this issue rises to the Supreme Court, the Court should adopt the particularity approach.

V. IMPLICATIONS OF THE PARTICULARITY APPROACH AS THE LEADING APPROACH

If the particularity approach became the leading approach, the implications would be widespread. As the following sections discuss, the implications would reach courts, searchers, and, ultimately, electronic device users.

A. Implications for Courts

First, the Supreme Court's application of the particularity approach would impact lower courts. Courts that already utilize the particularity approach, such as the Sixth Circuit, the Eleventh Circuit, and the Court of Appeals for the Armed Forces, would continue to interpret the scope narrowly and preserve the expectation of privacy in electronic devices, while adapting the particularity approach to accommodate further developments in technology yet unknown. However, courts that use the container approach or that have yet to address the issue would need to examine existing applications of the particularity approach, consider the unique characteristics and privacy concerns of electronic devices, and implement the particularity approach as the superior approach.

If the issue progressed to the Supreme Court and the Court applied the particularity approach, the ruling would have constitutional force. By way of the Supremacy Clause, such a ruling would compel lower courts to adopt the particularity approach.[324] This domino effect would squash potential resistance from courts, such as the Fifth and Seventh Circuits, that might continue to favor the container approach.

---

323 *See Kyllo*, 533 U.S. at 41 (Stevens, J., dissenting).

324 *See* U.S. CONST. art. VI.

B. Implications for Searchers

Second, application of the particularity approach as the leading approach would change the behavior of searchers. The majority of private searchers are likely not aware of changes in Fourth Amendment doctrine; thus, in all probability, they would not alter their search behavior to accommodate the particularity approach. However, government officials would presumably be conscious of such an instrumental change in Fourth Amendment doctrine and may alter their search behavior in response.

The particularity approach requires government officials to limit their government searches to material actually viewed during the private search.[325] This principle might trigger changes in search behavior, as the more a private searcher actually views, the more government officials can search without a warrant. Thus, law enforcement officers might urge private searchers to conduct the broadest searches possible to maximize the material the government can warrantlessly search. However, these searchers would likely lose their qualifications as private searchers because they acted as "instruments" of the government.[326] The danger of this label is that any evidence obtained by these "instruments" would be suppressed as the product of an unreasonable search.[327] This potential suppression of evidence would create an incentive for instructing government officials and searchers to commit perjury in an attempt to hide the true nature of the search and prevent suppression of the evidence.[328] While this would be a potential danger to be aware of, law enforcement agencies could combat such an incentive to commit perjury by implementing additional oversight programs and raising awareness of the consequences of perjury.

Another implication of the particularity approach is that government officials might change their search conduct to stay within the narrow scope permitted by the particularity approach. The particularity approach's narrow scope requires government officials to exercise caution when conducting their subsequent searches in order to avoid exceeding the scope. The consequence of

---

325 *See* United States v. Wicks, 73 M.J. 93, 100–01 (C.A.A.F. 2014).

326 *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

327 *See supra* notes 39–40, 53–54 and accompanying text.

328 *See* Dripps, *supra* note 39, at 1 (explaining that the exclusionary rule has been criticized as "fostering police perjury and judicial hypocrisy"); *see also* L. Timothy Perrin, H. Mitchell Caldwell & Carol A. Chase, *It is Broken: Breaking the Inertia of the Exclusionary Rule*, 26 PEPP. L. REV. 971, 988–89 (1999) (explaining that police have been shown to "lie in order to prevent exclusion of evidence" and that "police perjury is fostered by the exclusionary rule").

failing to exercise the requisite caution is the resulting evidence's exclusion from the prosecution's case in chief pursuant to the exclusionary rule.[329] Thus, the particularity approach may increase the burden on government officials to stay within the narrow scope of the private search and precipitate changes in search conduct to avoid the outcome of suppression. However, the public benefit in protecting individuals' private information from permissive government searches overshadows the increased burden on police officers to stay within the literal scope of the private search.

C. Implications for Electronic Device Users

Finally, the implications of the particularity approach extend to every user of electronic devices. The *Riley* case stressed the pervasiveness of electronic devices in our day-to-day lives when it reported that "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[330] These 90% of American adults who own a cell phone, and the vast majority who own other forms of electronic devices, all have a stake in preserving their privacy interests in digital records, "from the mundane to the intimate."[331] Therefore, they have an interest in the privacy rights that the particularity approach strives to protect.

More importantly, every electronic device user would be affected by the particularity approach because it protects all users against intrusive government searches. The particularity approach emphasizes the necessity of a narrow scope to prevent government officials from viewing legal, but private, information.[332] Thus, the particularity approach protects the privacy of everyone—innocent or otherwise—from prying government intrusions into private information, as the Fourth Amendment intends.[333]

CONCLUSION

Electronic devices pose unique issues that historic private search doctrine jurisprudence does not address. Despite attempts to analogize electronic devices to traditional containers, trying to compare something as unique as an

---

329 *See supra* notes 39–40, and accompanying text.
330 Riley v. California, 134 S. Ct. 2473, 2490 (2014).
331 *See id.*
332 *See* United States v. Lichtenberger, 786 F.3d 478, 488–89 (6th Cir. 2015).
333 *See id.*

electronic device to something as static as a traditional container is an impractical task.[334] On the other hand, the particularity approach utilizes a narrow scope and limits the subsequent government search to what the private searcher viewed.[335] In so doing, the particularity approach accommodates the unique characteristics of electronic devices. Thus, the particularity approach is the superior approach to determining the scope of a private search in the context of electronic devices. Therefore, courts should implement the particularity approach, and, if the issue rises to the Supreme Court, the Court should adopt the particularity approach. The implications of the Court utilizing the particularity approach would be widespread, with courts, searchers, and electronic device users all experiencing the impact. Despite the many positive changes that the particularity approach would precipitate, the most vital attribute of the particularity approach is its commitment to preserving privacy in a technological era. "Privacy is not insignificant; it is not something to be taken for granted; and even as it diminishes as our world becomes more interconnected and dangerous, privacy must not become a legal fiction."[336] To prevent privacy from becoming a memory, courts must adopt the particularity approach and prevent intrusive government invasions.

ALEXANDRA GIOSEFFI*

334 *See* United States v. Wicks, 73 M.J. 93, 102 (C.A.A.F. 2014) (arguing that analogizing electronic devices to containers does not take into account the unique issues associated with electronic devices).

335 *See id.* at 100–01.

336 State v. Subdiaz-Osorio, 849 N.W.2d 748, 760 (Wis. 2014).

* Notes & Comments Editor, *Emory Law Journal*; J.D., Emory University School of Law (2017); B.S., University of Florida (2013). I would like to thank my comment advisor, Professor Morgan Cloud, for his guidance and support during this process. I would also like to thank the outstanding editors of *Emory Law Journal*, particularly Nathan North and Grace Zoller, whose keen eyes and diligent editing were invaluable in preparing this Comment for publication. Thank you to my grandparents for teaching me the importance of perseverance and hard work. To my sister, Anna, who is the greatest supporter and friend one could ask for. Finally, thank you to my parents, John and Robyn Gioseffi, for supporting me in all of my endeavors and for always encouraging me to reach further.