Texas A&M Law Review

Volume 4 | Issue 2

9-18-2017

Lichtenberger and The Three Bears: Getting the Private Search Exception and Modern Digital Storage "Just Right"

Samuel Crecelius

NOTE

LICHTENBERGER AND THE THREE BEARS: GETTING THE PRIVATE SEARCH EXCEPTION AND MODERN DIGITAL STORAGE "JUST RIGHT"

*by Samuel Crecelius**

TABLE OF CONTENTS

I. INTRODUCTION

Finding a happy medium is hard. Often, it is a challenge to find a workable balance between two unworkable extremes. Known as the "Goldilocks Principle," this phenomenon has been observed in fields as diverse as developmental psychology and astrobiology.[1] As Goldilocks found in the Three Bears' house, "just right" may not come on the first attempt. We may have to explore the extremes of the spectrum—"too hot" and "too cold"—before we can settle on "just right."

* J.D. Candidate, Texas A&M School of Law.

1. *Goldilocks Principle*, WIKIPEDIA, THE FREE ENCYCLOPEDIA, https://en.wikipedia.org/wiki/Goldilocks_principle [https://perma.cc/XJ93-Z4T9] (last visited July 24, 2016).

DOI: https://doi.org/10.37419/LR.V4.I2.3

Goldilocks also discovered that this process is all the more difficult in a new environment—like the Three Bears' house. Goldilocks persevered, however, until she found "just right."

Federal courts face a similar dilemma in the private search exception to warrant requirements under the Fourth Amendment. On one hand are legitimate individual privacy interests and on the other, the legitimate interests of law enforcement to protect society. Courts must not handcuff law enforcement agents in their duties in the name of individual privacy ("too cold"), but neither should they unreasonably curtail individual liberty by giving too much latitude to legitimate government interests ("too hot"). It is no small task to identify an appropriate compromise between the competing principles of protecting the privacy of American citizens and protecting American citizens from crime. Like Goldilocks, courts today also face this challenge in an unfamiliar world. What is the "just right" application of the private search exception in the world of digital storage devices, which hold staggeringly large amounts of data and whose structure challenges traditional Fourth Amendment concepts?

The Fourth Amendment directs that:

> 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.[2]

The Supreme Court has developed a two-part test to determine whether law enforcement violates this requirement of the Fourth Amendment.[3] First, the Court asks whether the law enforcement action constitutes a "search."[4] The action is only a Fourth Amendment search "when the government violates a subjective expectation of privacy that society recognizes as reasonable."[5] If the government conducted a search, the Court then decides whether the search was reasonable—by its text, the Fourth Amendment forbids the government from "unreasonable" searches.[6] Outside of certain specific exceptions, warrantless searches are *per se* unreasonable.[7] If there is no "search," therefore, the reasonableness of the act is not an issue—and no warrant is required.

---

2. U.S. CONST. amend. IV.

3. *See* Kyllo v. United States, 533 U.S. 27, 31–33 (2001).

4. *Id.* (analyzing the "antecedent question of whether or not a Fourth Amendment 'search' has occurred").

5. *Id.* at 33 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

6. U.S. CONST. amend. IV.

7. City of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015) (quoting *Katz*, 389 U.S. at 357).

The distinction between what is and is not a search comes to the fore when private citizens disclose information to the police. Under these circumstances, courts apply the so-called "private search doctrine." The Fourth Amendment applies only to government action.[8] A private party's act, therefore, can never be a "search" under Fourth Amendment analysis, no matter how unreasonable[9] or unlawful.[10] Under the private search doctrine, law enforcement may recreate a third party's investigation without triggering a Fourth Amendment "search" so long as they do not exceed the scope of the private search.[11] If law enforcement stays within the scope of the private search, therefore, they do not require a warrant.[12] However, if law enforcement exceeds the scope of the private search, they initiate a Fourth Amendment search, and must obtain a warrant[13] or have the fruits of their search excluded at trial.[14]

In practice, courts commonly define the scope of a private search in terms of containers—from brown paper bags[15] to luggage[16] to camera lens cases.[17] Unless previously opened by a private party, each new container opened triggers a new search by law enforcement.[18] In some cases, a private party might look through only some of the contents of a container before turning it over to the police. The police, however, may search deliberately and exhaustively through that container.[19]

8. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (citing United States v. Jacobsen, 466 U.S. 109, 113–14 (1984)).

9. *Jacobsen*, 466 U.S. 109 at 114–15.

10. *See, e.g.*, United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003) (permitting government use of information illegally hacked by a private party); United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003) (permitting the same).

11. *See Jacobsen*, 466 U.S. at 119 ("it hardly infringed respondents' privacy for the agents to re-examine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube"); United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990) (federal agents did not exceed the scope of prior private search "simply because they took more time and were more thorough than [the private party]").

12. *Jacobsen*, 466 U.S. at 117–18 (stating that a "search" takes place "only if the authorities use information with respect to which the expectation of privacy has not already been frustrated"). *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014) (noting that warrantless searches are presumptively unreasonable).

13. *Jacobsen*, 466 U.S. at 117–18.

14. *See* Mapp v. Ohio, 367 U.S. 643, 648 (1961) (citing Wolf v. Colorado, 338 U.S. 25, 28 (1949)). *But see* Herring v. United States, 555 U.S. 135, 141 (2009) (stating the exclusionary rule applies "only where it 'result[s] in appreciable deterrence' ").

15. *See, e.g.*, Smith v. Ohio, 494 U.S. 541, 541–42 (1990) (per curiam).

16. *See, e.g.*, United States v. Place, 462 U.S. 696, 706–07 (1983).

17. *See, e.g.*, United States v. Donnes, 947 F.2d 1430, 1435–36 (10th Cir. 1991).

18. *See id.* at 1438 (a container's contents are typically only revealed by opening it, not based on its "incriminating character"); United States v. Kinney, 953 F.2d 863, 866 (4th Cir. 1992) (police's search of a small white bag in a closet not supported by a private party's opening other bags in the closet); United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001) ("police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers . . . .").

19. *See* United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990) (sanctioning a federal search of a container already opened by a private party even though federal agents "took more time and were more thorough than [the private party]").

Courts have historically treated digital storage devices as simply another form of container.[20] In the modern world, however, private information is more and more likely to be stored in digital form, and storage devices for such information grow larger and larger. Therefore, as the application of the private search doctrine in the context of the digital world is becoming more commonplace, the significance of correctly applying the doctrine is increasingly heightened. It is exceptionally important, therefore, that courts apply the private search doctrine "just right"—restrictively enough to protect personal privacy while applying it liberally enough to further the legitimate goals of law enforcement.

On this spectrum of personal privacy and law enforcement, courts have tended to gather at the extremes. Most courts have treated the digital storage device as a unitary container. This approach has come to apply the private search doctrine so broadly that it endangers the right to privacy embodied by the Fourth Amendment. On the other extreme stands the Sixth Circuit, who most recently considered this issue in *United States v. Lichtenberger*.[21] Although the Sixth Circuit did not explicitly address the container doctrine, the court impliedly limited the container to the individual file. The court held that an officer exceeded the private search's scope because he could not be certain that he viewed only those files that the private party viewed.[22] The Sixth Circuit settled firmly on the restrictive end of the spectrum in resolving this issue.[23] In the interest of protecting individual privacy, however, the Sixth Circuit's decision will hamstring law enforcement and effectively obliterate the private search doctrine in the digital context. How courts resolve the issue of digital container size in future decisions will largely shape the fate of the private search doctrine in the digital world.

This Note recommends a third option to analyze warrantless police searches under the private search doctrine. Specifically, courts should define the container as the virtual file folder (or folders) containing the data actually viewed by the private searcher. This "just right" approach avoids both the "too hot" traditional approach and the "too cold" of the strict approach. A virtual file folder concept would appro-

20. *Runyan*, 275 F.3d at 458 (assuming without deciding that computer disks are Fourth Amendment containers because neither party contested the point); Rann v. Atchison, 689 F.3d 832, 836–37 (7th Cir. 2012) (adopting *Runyan*'s approach to digital storage devices); United States v. Harling, No. 2:13-cr-96-FtM-38CM, 2014 U.S. Dist. LEXIS 107398, at *9–10 (M.D. Fla. Aug. 4, 2014) (identifying thumb drives as closed containers).

21. United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015). In fact, it may be one of the only circuits to consider the issue in the last ten years. *See Runyan*, 275 F.3d 449.

22. *Lichtenberger*, 786 F.3d at 488–89.

23. Interestingly, the Sixth Circuit held that the police search exceeded the scope of the private search *because* of the vast potential privacy interest at risk. It is not clear that this is the appropriate way to consider the issue.

priately guard individual privacy rights while preserving law enforcement's ability to utilize volunteered evidence. Such a middle ground would additionally provide courts with discretion to expand or restrict the scope of the private search as the circumstances warrant, consistent with the fact-intensive "reasonableness" criteria of the Fourth Amendment.[24]

Part II of this Note reviews the history of the private search exception to the Fourth Amendment warrant requirement and its place within the historical goals of Fourth Amendment jurisprudence, as well as the relevant background of modern computer technology. In Part III, this Note looks at current applications of the private search doctrine to digital storage, noting difficulties with each approach. Finally, in Part IV, this Note recommends an appropriately balanced approach and responds to some potential counterarguments.

II. Background

A. *The Private Search Exception*

The Supreme Court has consistently construed the Fourth Amendment as inapplicable to citizens acting in their individual capacities.[25] Instead, the Fourth Amendment prohibits government actors (federal agents as well as state and local law enforcement) from conducting unreasonable searches and seizures.[26] This limitation on the application of the Fourth Amendment leads naturally to what is known as the private search exception. Law enforcement may utilize information volunteered by third parties even if obtained under circumstances that would have violated the Fourth Amendment had law enforcement conducted the search.[27] Thus, the Fourth Amendment does not apply "to a search or seizure, even an unreasonable one, effected by a private individual" so long as the private party is truly acting in a private capacity and not as an agent of the state or with its sanction.[28]

Law enforcement may not use a private party's search, however, to frustrate the underlying purpose of the Fourth Amendment—preventing general searches.[29] If a private party performs an exhaustive search, law enforcement may utilize all of that information.[30] How-

24. *See, e.g.*, discussion *infra* Section IV.B.1.

25. United States v. Jacobsen, 466 U.S. 109, 113 (1984); Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

26. *See* Wolf v. Colorado, 338 U.S. 25, 27–28 (1949) (holding the Fourth Amendment applicable to the states through the Fourteenth Amendment's Due Process Clause).

27. *Jacobsen*, 466 U.S. at 117.

28. *Id.* at 113–14 (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).

29. *See infra* Section II.A.1.

30. *See* United States v. Odoni, 782 F.3d 1226, 1240 (11th Cir. 2015) (applying the private search doctrine to a search by the British government and upholding the admission of all evidence because the British search was exhaustive).

ever, the government may not use a private search as an excuse to conduct its own general search.[31] Faithful to the spirit of the Fourth Amendment,[32] the private search exception allows for only *limited* searches.

In *United States v. Jacobsen*, the Supreme Court laid the foundation for the private search exception as it is applied today. Federal Express ("FedEx") employees examined a damaged package at their Minneapolis-St. Paul office.[33] Inside, they discovered a tube, which a manager cut open to reveal three zip-lock plastic bags containing white powder.[34] The manager and employees called the DEA after placing the plastic bags back in the tube and the tube back in the damaged box.[35] When the DEA agent arrived, he removed the tube from the open box and the zip-lock bags from the tube.[36] The agent also field-tested each of the bags, determining that the white powder in each was cocaine.[37] The DEA obtained and executed arrest warrants on the intended recipients of the package.[38] At trial, the defendants moved to suppress the evidence as the result of an illegal search and seizure.[39]

The Supreme Court held that the DEA agent's actions at the FedEx office were not subject to the Fourth Amendment. The intended recipient of the package possessed a legitimate privacy interest in the package.[40] Although using information in which there is a legitimate, unfrustrated privacy interest implicates the Fourth Amendment,[41] any additional invasions beyond a private search "must be tested by the degree to which they exceeded the scope of the private search."[42] In *Jacobsen*, the DEA agent merely protected against the risk that a third party misdescribed the contents of an unsealed container searched by the third party and made freely available to law enforcement.[43] Any legitimate privacy interest in the package had been frustrated by the private search.[44] The DEA agent's acts, therefore, did not violate the Fourth Amendment.[45] The DEA had not conducted a "search" for the purposes of the Fourth Amendment. Finally, the

31. *See infra* Section II.A.1.
32. *See infra* Section II.A.1.
33. United States v. Jacobsen, 466 U.S. 109, 111 (1984).
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.* at 111–12.
38. *Id.* at 112.
39. *Id.*
40. *Id.* at 114; *see also* United States v. Ross, 456 U.S. 798, 822–23 (1982) (stating that "the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view").
41. *Jacobsen*, 466 U.S. at 117.
42. *Id.* at 115.
43. *Id.* at 119.
44. *Id.* at 121.
45. *Id.*

Court held that the field test on the white powder in the zip-lock bags did not infringe a legitimate privacy interest.[46] Although this field test did exceed the private search's scope,[47] the test could only reveal whether the white powder was contraband, and no other potentially private information.[48]

The private search exception can dramatically change the balance between government interests and a government intrusion into privacy. The Fourth Amendment protects citizens' expectations of privacy in matters "that society is prepared to consider reasonable."[49] But a private search can reduce or eliminate that reasonable expectation of privacy, thereby freeing law enforcement from Fourth Amendment constraints.[50] Under the private search exception, the court considers an individual's reasonable expectation of privacy *after* taking the private search into account.[51] In other words, given what a private party's search has revealed—is there any *remaining* reasonable privacy expectation? After a private search, it may be that a container "no longer support[s] *any* expectation of privacy."[52] Because it can dramatically reduce or completely eliminate an otherwise reasonable expectation of privacy, the private search exception to the Fourth Amendment is a powerful tool of law enforcement.

Since *Jacobsen*, courts apply the private search exception as a two-part test, balancing privacy interests against law enforcement interests.[53] First, the court determines whether the government search exceeded the scope of the original search[54]—unless the government agent exceeds the scope of the private search, there can be no Fourth Amendment "search."[55] If the government does exceed the scope of the private search, the court then examines the facts of the case to discover whether law enforcement infringed any remaining unfrustrated legitimate expectation of privacy following the private search.[56] The police are not prevented from utilizing information gathered from third parties,[57] therefore, because the owner of information discovered by or revealed to a third party no longer has a reasonable expec-

46. *Id.* at 123.
47. *Id.* at 122.
48. *Id.* at 122–23.
49. United States v. Lichtenberger, 786 F.3d 478, 482 (6th Cir. 2015) (quoting *Jacobsen*, 466 U.S. at 113).
50. *See Jacobsen*, 466 U.S. at 117.
51. *See id.* at 126 (stating that "federal agents did not infringe any constitutionally protected privacy interest that had not *already* been frustrated as the result of private conduct") (emphasis added).
52. *Id.* at 121 (emphasis added).
53. *See id.* at 122.
54. *Id.*
55. *See id.* at 113.
56. *Id.* at 115.
57. *Id.* at 117.

tation of privacy in it.[58] And it may be that the information revealed to the police will frustrate the owner's expectation of privacy in *other* information as well.[59] So, only if law enforcement exceeds the scope of the private search *and* infringes some still unfrustrated privacy interest will the evidence of the search be excluded. Thus, "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated."[60]

1. Containers and the Scope of the Private Search

The Fourth Amendment stands in defiance of general search warrants, which were sanctioned by the British monarchy before the American Revolution.[61] Under a general search warrant, the authorities were unrestricted in searching a person's belongings and effects.[62] Evidence thus discovered—even evidence of unsuspected crimes—could be used by the Crown against its owner.[63] In order to secure American citizens in their "persons, houses, papers, and effects,"[64] the Framers enacted the Fourth Amendment to limit government searches to the particular area and items described in a warrant.[65] This particularity requirement prevents general government searches.[66]

Consistent with this purpose, government action under the private search exception is similarly limited. The government must limit its searches to the scope of a previous private search.[67] Without this limit, government actors could take limited information provided by third parties and radically expand on that private search without obtaining a warrant based on probable cause. In other words, without this limitation, government actors would be able to use the private search doctrine to perform a general search. Limiting the scope of the government search thus serves the same purpose as the particularity requirement for warrant searches—protecting against a general search.[68]

---

58. *Id.*

59. *See generally id.* (discussing a private search of a package that revealed baggies of white powder and holding that under such circumstances the private search had removed any reasonable expectation of privacy in the contents of the baggies—later determined to be cocaine).

60. *Id.* at 117.

61. *See* Boyd v. United States, 116 U.S. 616, 624–25 (1886); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

62. *See* Stanford v. Texas, 379 U.S. 476, 481–82 (1965).

63. *See id.*

64. U.S. CONST. amend. IV.

65. *Id.*

66. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 565 (2005). *See Coolidge*, 403 U.S. at 467.

67. United States v. Lichtenberger, 786 F.3d 478, 482 (6th Cir. 2015) (citing United States v. Jacobsen, 466 U.S. 109, 116 (1984)).

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

The scope of a private search may be defined by reference to the "container doctrine"—the opening of a container by a private party frustrates the reasonable expectation of privacy with respect to the contents therein.[69] Because there is no Fourth Amendment "search" without a legitimate expectation of privacy, a private search of a container allows a state actor free access to the container.[70] A government agent is generally free to search—and search more thoroughly—the contents of a previously searched container without implicating the Fourth Amendment.[71]

The Fourth Amendment protects objects in which individuals have manifested an expectation of privacy "that society recognizes as reasonable."[72] A container manifests such an expectation, so long as the container "conceals its contents from plain view."[73] A broad spectrum of containers sufficiently conceal their contents to afford Fourth Amendment protection: purses;[74] briefcases;[75] duffel bags;[76] file folders;[77] and cardboard boxes.[78]

When applying the Fourth Amendment, opening each distinct container is a new "search" for the purposes of the court's analysis.[79] An independent search begins when the government agent further invades the property owner's interest.[80] Contents of a closed container typically demonstrate a reasonable expectation of privacy,[81] and thus require an independent justification to overcome the safeguards of the

69. *Jacobsen*, 466 U.S. 109 (1984). *See* United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990) (stating that a more thorough search of a container already opened by a private party does not exceed the scope of a private search). *See also* United States v. Kinney, 953 F.2d 863 (4th Cir. 1992) (finding that police did not exceed the scope of a private search when going through a bag of firearms previously opened by the owner's girlfriend, but the police did exceed the scope of that private search when they opened a second bag in the same closet which the girlfriend had not previously opened). *But see* United States v. Rouse, 148 F.3d 1040 (8th Cir. 1998) (holding that police exceeded the scope of a private search when they examined all the contents of luggage partially searched by airline employees).

70. *See Jacobsen*, 466 U.S. 109 (1984) (stating that the expectation of privacy is frustrated to the extent that a third party has already searched, so a government action is not a "search" so long as it stays within the scope of the private search).

71. *Simpson*, 904 F.2d at 610.

72. Kyllo v. United States, 533 U.S. 27, 33 (2001).

73. United States v. Ross, 456 U.S. 798, 822-23 (1982) (citing Robbins v. California, 453 U.S. 420, 427 (1981) (plurality opinion)).

74. *E.g.*, United States v. Welch, 4 F.3d 761, 764 (9th Cir. 1993).

75. *E.g.*, United States v. Basinski, 226 F.3d 829, 838 (7th Cir. 2000).

76. *E.g.*, Bond v. United States, 529 U.S. 334, 336 (2000).

77. *E.g.*, United States v. Knoll, 16 F.3d 1313, 1321 (2d Cir. 1994).

78. *E.g.*, United States v. Fultz, 146 F.3d 1102, 1105 (9th Cir. 1998).

79. *See* United States v. Runyan, 275 F.3d 449, 462–63 (5th Cir. 2001) (citing United States v. Kinney, 953 F.2d 863, 866 (4th Cir. 1992)); United States v. Donnes, 947 F.2d 1430, 1436 (10th Cir. 1991).

80. Arizona v. Hicks, 480 U.S. 321, 325 (1987).

81. Robbins v. California, 453 U.S. 420, 426 (1981) (plurality opinion) (quoting United States v. Chadwick, 433 U.S. 1, 11 (1977)).

Fourth Amendment.[82] A private party's search of a container, therefore, frustrates the privacy expectation in the items *within* the container, but not *without*.[83]

The container doctrine is often tied together with the concept that individuals cannot reasonably have a privacy expectation in items in "plain view."[84] By extension, neither can a container that "unmistakably reveal[s] its contents" sustain a reasonable expectation of privacy.[85] The contents of containers that are open, see-through, or have a distinctive character or shape are effectively in "plain view."[86] When a container declares its contents to the world, as it were, it cannot support a legitimate expectation of privacy.

Once a container is opened, however, the expectation of privacy is frustrated with respect to *all* of its contents, regardless of whether all the contents are technically exposed to "plain view." When a private party invites law enforcement to view an unsealed open container, there is no remaining privacy interest in that container.[87] Law enforcement may view what a third party has made available to them, therefore, without violating the Fourth Amendment.[88] Because the owner's expectation of privacy in an open container is frustrated, police may also take more time and search the container more thoroughly without implicating the Fourth Amendment.[89]

Within the context of a private search, this means that law enforcement searches are restricted to the particular container searched by the private party. Evidence discovered through the efforts of a private party no longer retains a reasonable expectation of privacy, and therefore police examination of such evidence is not a "search" under the Fourth Amendment. But the contents of a still-unopened container retain that reasonable expectation, in spite of physical proximity[90] or apparent culpability.[91]

---

82. *See* Walter v. United States, 447 U.S. 649, 657 (1980) ("[T]he Government may not exceed the scope of the private search unless it has the right to make an independent search.").

83. *But see infra* Section II.A.2.

84. *See* Arkansas v. Sanders, 442 U.S. 753, 764 n.13 (1979). *See also* United States v. Jacobsen, 466 U.S. 109, 131 (1984) (White, J., concurring in part and concurring in the judgment). *Cf.* United States v. Ross, 456 U.S. 798, 822–23 (1982) ("[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view.").

85. *Jacobsen*, 466 U.S. at 129 (White, J., concurring in part and concurring in the judgment) (citing *Ross*, 456 U.S. at 822–23).

86. United States v. Williams, 41 F.3d 192, 197 (4th Cir. 1994) (quoting United States v. Corral, 970 F.2d 719, 725 (10th Cir. 1992)).

87. *Jacobsen*, 466 U.S. at 121.

88. *Id.* at 119–20 (first citing Coolidge v. New Hampshire, 403 U.S. 443, 487–90 (1971); then citing Burdeau v. McDowell, 256 U.S. 465, 475–76 (1921)).

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

90. *See* United States v. Kinney, 953 F.2d 863, 866 (4th Cir. 1992).

91. *See* United States v. Donnes, 947 F.2d 1430, 1439 (10th Cir. 1991) (holding that a closed camera lens case still exhibited a reasonable expectation of privacy, although

2. Remaining Unfrustrated Expectation of Privacy

The Fourth Amendment inquiry does not end by determining that law enforcement has exceeded the scope of a private search. Unless the property owner still retains some expectation of privacy that society is prepared to consider reasonable, a search beyond the scope of that private search (for the purposes of this Note, beyond the confines of the container) would not violate the Fourth Amendment.

Jacobsen provides a clear example of the frustration-of-privacy expectation beyond the scope of the private search. The Supreme Court described this as "virtual certainty" about the subject of the additional search.[92] There, FedEx employees searched a damaged package pursuant to company policy.[93] After opening the cardboard box wrapped in brown paper, the employees discovered a tube beneath layers of newspaper.[94] Inside this tube were several plastic bags full of white powder.[95] After the employees contacted the DEA, an agent opened the plastic bags, which had not been opened by the FedEx employees, and determined by field test that the powder inside was cocaine.[96]

The Court held first that the agent's reexamination of the package did not violate the Fourth Amendment because the agent could be virtually certain of the packages contents based on the employees' comments to the agent.[97] Therefore the agent "merely avoid[ed] the risk of a flaw in the employees' recollection," instead of infringing any remaining reasonable expectation of privacy.[98] Secondly, the Court held that the agent's field test of the white powder contained in the package was reasonable based on employee statements, the circumstances of the search, and the agent's expertise.[99] "[T]he package could no longer support any expectation of privacy" and therefore the agent did not violate the Fourth Amendment in exceeding the scope of the employees' search.[100] *Jacobsen* provides very straightforward examples of circumstances in which an otherwise reasonable expectation was nullified. In other cases involving both physical and digital searches, however, courts have identified a variety of circumstances in which a party's reasonable expectation of privacy was lessened or eliminated.[101]

---

it was found in a glove along with a syringe, giving the officer only a "strong basis to infer" that the case contained contraband).

92. *Jacobsen*, 466 U.S. at 119.
93. *Id.* at 111.
94. *Id.*
95. *Id.*
96. *Id.* at 111–12.
97. *Id.* at 119.
98. *Id.*
99. *Id.* at 121.
100. *Id.* at 121–22.
101. *See* United States v. Harling, No. 2:13-cr-96-FtM-38CM, 2014 U.S. Dist. LEXIS 107398, at *12 (M.D. Fla. Aug. 4, 2014) (holding that a private party's discovery of child porn on two thumb drives and claim that they had seen child porn on a

Elaborating on *Jacobsen*, the Fifth Circuit explained that the reasonable expectation of privacy in a container's contents could be frustrated based on "the statements of the private searchers, [law enforcement's] replication of the private search, and their expertise."[102] Alternatively, if an unopened container's "contents were rendered obvious by the private search," then the police may be "substantially certain" of the contents of the container, and opening the container would not violate the Fourth Amendment.[103] In other words, "substantial certainty" is one—but not the only—way in which circumstances may frustrate any remaining privacy interest, thereby excusing law enforcement action from Fourth Amendment regulation.

B. *The Problem of Modern Digital Storage*

Technology seems to develop at an exponential pace. This may be best evidenced by the sheer space available for data storage. In 2014, Western Digital's subsidiary, HGST, released a ten terabyte hard drive for public sale[104]—an amount of storage equivalent to 647 million pages of Microsoft Word documents or almost 6.7 billion pages of plain text.[105] IBM's RAMAC was developed in the 1950s, in contrast, and stored approximately five *mega*bytes of data.[106] Weighing in at more than two thousand pounds, the RAMAC completely dwarfs hard drives today.[107] The shrinking size and growing capacity of digital storage has made it a mainstay in modern society. More than 80% of American households own a home computer of some type—more

third was sufficient to frustrate the owner's reasonable expectation of privacy in the third thumb drive); Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012) (affirming a thorough police search of digital storage devices delivered to the police by private parties based on the parties' description of the contents—child porn—without precise knowledge of the "scope" of the private search); United States v. Oliver, 630 F.3d 397, 407–08 (5th Cir. 2011) (holding the contents of a notebook delivered to the police were within the scope of the private search based on the title on the cover, a loose sheet of paper protruding from the side of the notebook, and the defendant's admission of his role in a fraudulent unemployment benefits scheme).

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

103. *Id.* at 463–64; *see also Rann*, 689 F.3d at 837–38.

104. Lucas Mearian, *WD Leapfrogs Seagate with World's Highest Capacity 10TB Helium Drive, New Flash Drives*, COMPUTERWORLD (Sept. 9, 2014, 12:05 PM), http://www.computerworld.com/article/2604311/computer-hardware/wd-leapfrogs-seagate-with-world-s-highest-capacity-10tb-helium-drive-new-flash-drives.html [https://perma.cc/3APZ-443U].

105. *How Many Pages in a Gigabyte?*, LEXISNEXIS, https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf [https://perma.cc/Q6CM-6SMX] (last visited Feb. 24, 2016).

106. *Tech Time Warp of the Week: The World's First Hard Drive, 1956*, WIRED (Jan. 3, 2014, 9:30 AM), http://www.wired.com/2014/01/tech-time-warp-ibm-ramac/ [https://perma.cc/NHC3-MK34].

107. *Id.*

than 90% of householders are under the age of 45.[108] "Smartphones" are nearly as ubiquitous, with more than 60% of American adults owning one.[109] That means that some 150 million Americans walk the streets each day with handheld devices, many of which have more than three *thousand* times the capacity of the RAMAC.[110] What once would have required an entire library[111] is now contained in a two-pound block measuring 7 x 4.5 x 1.5 inches.[112]

In spite of their popularity, hard drives' inner workings remain unknown to many people. Similar to cassette tapes of an earlier era, hard drive storage operates through magnetism.[113] The drive consists of one or more "platters," on which an electronic arm reads and writes data.[114] Each platter is segmented into distinct tracks containing smaller sectors.[115] "Importantly, for purposes of the Fourth Amendment analysis, '[w]hen a file is written to a hard [drive] it is not written in consecutive sectors. Sectors are scattered all over the disk, organized as a linked list.'"[116] In the physical world, items stored in the same container will have a certain level of proximity to each other. On a hard drive, however, documents stored in the same folder may or may not be written to adjacent sectors.

The Supreme Court has noted that exceptions to the Fourth Amendment warrant requirement are analyzed in light of the "legitimate governmental interests," and the degree to which a search intrudes an individual's privacy on the other.[117] The relative weight of these interests in a given case factors substantially in the Court's decision. For instance, after a lawful arrest an officer may search the arres-

108. Thom File & Camille Ryan, *Computer and Internet Use in the United States: 2013*, U.S. CENSUS BUREAU 2–3 (Nov. 2014), http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf [https://perma.cc/HG7Z-BPF8].

109. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ [https://perma.cc/QA3J-VX3L].

110. *See* Georgia Dow, *16GB, 32GB, or 64GB: Which iPhone 5 Storage Size Should You Get?*, IMORE (Sept. 13, 2012, 5:22 PM), http://www.imore.com/16gb-32gb-or-64gb-which-iphone-5-storage-size-should-you-get [https://perma.cc/P4CY-CDAB]. *Cf.* WIRED, *supra* note 106.

111. *See* Kerr, *supra* note 66, at 542 (equating eighty gigabytes—one-twelfth of one terabyte—to one floor of a library).

112. *Seagate Expansion 5TB Desktop External Hard Drive USB 3.0*, AMAZON.COM, http://www.amazon.com/Seagate-Expansion-Desktop-External-STEB5000100/dp/B00TKFEEBW/ref=sr_1_1?ie=UTF8&qid=1456342713&sr=8-1&keywords=5tb [https://perma.cc/56PW-RRHK] (last visited Feb. 24, 2016).

113. Marshall Brain, *How Hard Disks Work*, HOWSTUFFWORKS: TECH, http://computer.howstuffworks.com/hard-disk.htm/printable [https://perma.cc/DEB9-KTJK].

114. *Id.*

115. *Id.*

116. Marc Palumbo, *How Safe is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 989 (2009) (quoting Stephen J. Rogowski, *Hard Disk*, *in* CONCISE ENCYCLOPEDIA OF COMPUTER SCIENCE 357 (Edwin D. Reilly ed., 2004)).

117. Riley v. California, 134 S. Ct. 2473, 2484 (2014).

tee's person and the area within the arrestee's control without a warrant.[118] Protecting the officer from concealed weapons and identifying evidence which the arrestee might attempt to destroy weigh heavily in favor of the government's legitimate interests.[119] Further, in a search incident to arrest, the arrestee's reasonable expectation of privacy is greatly reduced. The Supreme Court has noted that an arrestee's privacy interest is greatly diminished by the state's establishment of "dominion" over him.[120] With a substantial law enforcement interest on one side and a reduced privacy interest on the other, searches incident to arrest have become so commonplace that they are the norm rather than a Fourth Amendment exception.[121]

The balance appears to have shifted, however, when the object of the search involves digital storage—such as a search of an arrestee's phone.[122] Law enforcement interests, on one hand, are significantly reduced in the case of a smartphone. The arrestee cannot not use the data on his or her phone as a weapon, or to resist arrest.[123] And once the phone is confiscated there is minimal further risk of lost or destroyed evidence.[124] On the other side of the scale, a modern smartphone's vast capacity for potentially private data changes the weight of the arrestee's privacy interest, otherwise diminished by the arrest itself.[125] When so much personal information is involved, there is a much higher privacy interest in the data. A slip of paper with an accomplice's number on it is much easier to destroy than a complete 12-month conversation history stored as texts in a smartphone. At the same time, the conversation history stored on a phone reveals a great deal more private information than a simple slip of paper. When dealing with digital storage devices, individual privacy interests are heightened while law enforcement interests in searching the device may be diminished.

The modern complexity of digital storage presents conceptual challenges to courts. In *United States v. Crist*, one district court approached the private search doctrine by analyzing the literal segments of the hard drive "platters" accessed by the government agent.[126] This approach is problematic as applied to subsequent recreations of private searches because the virtual display of the storage device—the visible "file folders"—may give no indication which portions of the drive have been accessed.[127] Further, because a file is not written to

118. United States v. Robinson, 414 U.S. 218, 224 (1973).
119. *Id.* at 225 (quoting Chimel v. California, 395 U.S. 752, 762–63 (1969)).
120. *Id.* at 232 (quoting People v. Chiagles, 142 N.E. 583, 584 (1923)).
121. *Riley*, 134 S. Ct. at 2482.
122. *Id.* at 2484.
123. *Id.* at 2484–85.
124. *Id.*
125. *Id.*
126. United States v. Crist, 627 F. Supp. 2d 575, 586 (M.D. Pa. 2008).
127. *See* Palumbo, *supra* note 116, at 989.

the hard drive in consecutive sectors, but is "scattered all over the disk," data from a single file may be stored on multiple platters.[128] Attempting to treat each platter as a closed container, as *Crist* urges, would likely require a forensic review of the disk, meaning that law enforcement would have to exceed the scope of the private search (by conducting a complete scan of the drive) just to determine the scope of the private search. Otherwise, a government agent attempting to recreate a private search would be working blind, with no idea whether he or she may exceed the scope of the private search and virtually ensuring a later finding of unreasonable search and/or seizure.

It appears the only other way to ensure that a subsequent search does not exceed the scope of a private search would be for the government agent to limit the subsequent search to the precise data already accessed. Even if this would restrict the "search" to the previously accessed sections of the hard drive, this would merely be the "too cold" interpretation of *Lichtenberger* in another guise, falling prey to the same pitfalls.[129]

Further undermining its use in the private search context, this technical approach is unworkable as a practical matter under virtually any aspect of the Fourth Amendment—a warranted search as well as the exceptions. Law enforcement could scarcely describe an intended search with particularity if they had to describe "such and such portion of one platter, and such and such portions of three other platters." Unlike, say, reports that a suspect has cocaine in the trunk of his car, it is practically inconceivable that a warrant request could identify that a suspect had pirated music files on particular physical portions of a drive without a prior forensic search. What remains is to determine what the appropriate approach to digital storage *is*, if a literal or technical approach is inapt.

III. "Too Hot" and "Too Cold"

There are two principal ways to address the container doctrine as applicable to digital storage devices. In the early stages of digital storage, courts treated disks as single containers and maintained this approach as digital storage developed. *United States v. Runyan* is an example of this traditional, "too hot" approach.[130] The development of digital storage technology since *Runyan* has left its container approach unworkable. In 2015, the Sixth Circuit decided *United States v. Lichtenberger*.[131] There, the court effectively limited the digital "container" to the individual data file.[132] This new, "too cold" ap-

128. *Id.*
129. *See infra* Section III.B.
130. *See* United States v. Runyan, 275 F.3d 449 (5th Cir. 2001).
131. *See* United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015).
132. *Id.*

proach addresses the privacy concerns of modern digital storage by strictly limiting the scope of a government search in the digital context. This approach is also unworkable because it effectively prevents law enforcement from doing their job. After reviewing both the "too cold" and "too hot" approaches, the reader can better understand the need for a moderate, "just right" approach.

A. *"Too Hot"*

Treating each digital storage device or hard drive as a distinct and singular container is perhaps the most "common sense" approach to digital storage devices and the private search exception. Each device—thumb drive, zip drive, or computer—holds "x" data, so it makes sense on a surface level to treat those bits of data as individual items in a container. Many, if not most, federal courts have applied and continue to apply this traditional approach.[133]

In *United States v. Runyan*, the Fifth Circuit applied the private search exception in the context of digital storage.[134] It is perhaps the seminal example of a court considering digital storage and the container doctrine. After Runyan filed for divorce from his wife Judith, she returned to Runyan's ranch home to collect her personal property.[135] Judith and a friend scaled a fence surrounding the ranch and entered the home through a window.[136] There the women discovered a black duffel bag and ammunition boxes in Runyan's barn.[137] The duffel bag and ammunition boxes contained a variety of pornographic items, including a polaroid of an apparent minor.[138] While searching the rest of Runyan's ranch, Judith also found a desktop computer, which she claimed belonged to her, "surrounded by 3.5 inch floppy disks, CDs, and ZIP disks."[139] A friend of Judith reassembled the computer at Judith's residence and viewed "approximately twenty" CDs and floppy disks.[140] After finding images of child pornography, Judith's friend contacted the sheriff's department and

133. *See, e.g.*, United States v. Harling, No. 2:13-cr-96-FtM-38CM, 2014 U.S. Dist. LEXIS 107398 (M.D. Fla. Aug. 4, 2014) (treating a thumb drive as a container, allowing the police to review its contents more exhaustively than did the private party); Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012) (treating a memory card and zip drive as containers, allowing police to thoroughly review its contents without inquiring whether the private party had seen all the contents); United States v. Odoni, 782 F.3d 1226 (11th Cir. 2015) (treating a thumb drive as a single container); *Runyan*, 275 F.3d 449 (5th Cir. 2001) (computer floppy disks). *But see* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (distinguishing modern storage devices from traditional physical containers such as filing cabinets).

134. *Runyan*, 275 F.3d 449 (5th Cir. 2001).

135. *Id.* at 452.

136. *Id.* at 453.

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

turned over more than forty of these storage disks.[141] Judith and her friend viewed only some of the disks and looked at only some of the images on those disks.[142] Law enforcement viewed at least several images from each disk.[143] The trial court denied Runyan's motion to suppress this evidence[144] and Runyan was convicted of child pornography charges.[145] The Fifth Circuit addressed Runyan's argument on appeal that the police had exceeded the scope of the prior private search.[146]

The Fifth Circuit applied the container doctrine to be logically consistent with prior cases and to make a workable rule in real-world practice. The court first agreed that Runyan had a legitimate expectation of privacy in the computer disks.[147] Two questions then needed an answer: whether police exceeded the scope of the private search when they examined the entire collection of disks while the private searchers had examined only some of the disks; and whether police exceeded the scope of the private search when they examined more items on a particular disk that was opened by the private searchers.[148] Relying on *Jacobsen*, the Fifth Circuit held that police must have a warrant to open a closed container not opened by a private party, unless the police have substantial certainty about the contents of the container "based on the statements of private searchers, their replication of the private search, and their expertise."[149]

Because the police could not have been substantially certain about the contents of all the disks based only on the fact that all the disks were discovered in close proximity, the court found that the police had exceeded the scope of the private search with respect to disks not viewed by the private party.[150] With respect to disks which the private parties had viewed, however, the court found the police had not exceeded the scope of the private search.[151] The court reasoned that it "would not have been constitutionally problematic for the police to have examined more files than did the private searchers" under the container doctrine.[152] Reasoning that "an individual's expectation of privacy in the contents of a container has already been compromised if that container was opened and examined by private searchers," the court held that the police remained within the scope of the private search when they reviewed more items on an a disk than did the pri-

141. *Id.*
142. *Id.*
143. *Id.* at 454.
144. *Id.* at 455.
145. *Id.* at 452.
146. *Id.*
147. *Id.* at 458.
148. *Id.* at 461.
149. *Id.* at 463.
150. *Id.* at 464.
151. *Id.*
152. *Id.*

vate party.[153] Finding this approach most consistent with Fourth Amendment precedent, the Fifth Circuit adopted the approach that police could more thoroughly search digital containers in the same manner as physical containers, without violating the Fourth Amendment.[154]

The Fifth Circuit also found this approach to be the most practical. The alternative—an item-by-item comparison of the private search and police search—would result in "a warrantless "search" in violation of the Fourth Amendment each time [law enforcement] happened to find an item within a container that the private searchers did not happen to find."[155] The Fifth Circuit held instead that all of the data on those disks previously "opened" by a private searcher was admissible without a warrant.[156] In essence, the Fifth Circuit held that opening a digital container—like a physical container—exposes its contents to plain view, and therefore removes the contents' privacy expectation. Therefore, no new Fourth Amendment search had taken place.[157]

While this approach most closely resembles the physical world of containers in superficial respects, the ever-growing storage capacity created by modern technology ensures that this method tips the scales too far away from protecting private interests. When the police can gain access to a Library of Congress' worth of data completely without a warrant, based solely on a private party reviewing one or two images on the hard drive, for all practical purposes the police make a general search.

B. *"Too Cold"*

Some scholars have raised concerns about the potential vast amount of information exposed by application of the "traditional" approach to digital storage.[158] In 2015 the Sixth Circuit became the highest federal court to abandon the "traditional" approach to the container doctrine and digital storage for a stricter conceptualization—an individual-file-as-container approach.[159] This approach (by far the most restrictive

153. *Id.* at 464–65.
154. *Id.* at 464.
155. *Id.* at 465. *But see* United States v. Rouse, 148 F.3d 1040, 1041 (8th Cir. 1998).
156. *Runyan*, 275 F.3d at 465.
157. *Id.*
158. *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 203 (2005). *See also* Palumbo, *supra* note 116, at 980 (claiming that the traditional conceptualization of digital storage as a container is inapt in the digital world).
159. Orin Kerr, *Sixth Circuit Creates Circuit Split on Private Search Doctrine for Computers*, WASH. POST: VOLOKH CONSPIRACY (May 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers/?utm_term=.db9a898313d0 [http://perma.cc/UPW6-W6CT]. *See generally* United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015).

that has been suggested) avoids the challenges of a literal approach to the hard drive.[160] By limiting the scope of the private search to the precise data viewed by the private searcher, courts could avoid the problem that otherwise the visual display of files does not tell the viewer anything about where, physically, the data is stored in the device. It is perhaps an understandable reaction to the explosion of digital storage space in the modern era to guard individual privacy very closely.

However, this restrictive approach ignores the realities present in a private search situation and would ultimately nullify the private search doctrine with respect to digital storage. *Lichtenberger* itself provides a clear example of this fact. There, the defendant's girlfriend made an allegation to police that the defendant was in possession of child pornography, to which an officer responded.[161] Friends had warned her that defendant "had been previously convicted of child pornography offenses."[162] Police arrested Lichtenberger for failing to register as a sex offender after responding to his wife's request to escort him from their home.[163] In response to this shocking turn of events, the wife began to search Lichtenberger's personal laptop, which he would "never let [her] near."[164] The district court seems to describe her stumbling upon a handful of child pornography images after "hacking" Lichtenberger's laptop;[165] however, the circuit court notes that Lichtenberger's wife testified that "she viewed approximately 100 images of child pornography saved in several subfolders inside a folder entitled 'private.'"[166] Reading between the lines of the appellate case, it appears clear that the girlfriend reviewed a number of images in a hurry, most likely panicked at the discovery of such images.[167]

One of the officers who had responded to her original call returned to the house and asked Lichtenberger's girlfriend to show him what she had discovered.[168] Lichtenberger's girlfriend then began clicking on images at random.[169] She and the officer later testified they did not know if the images she showed him were the same images she saw in her initial search.[170] In essence, the Sixth Circuit held that the officer exceeded the scope of the private search, because the girlfriend was

160. *See supra* Section II.B.
161. *Lichtenberger*, 786 F.3d at 480.
162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.* ("The laptop was password protected, but Holmes hacked the laptop by running a password recovery program.").
166. *Id.* at 481.
167. *Id.*
168. *Id.* at 480.
169. *Id.*
170. *Id.* at 488–89.

unable to precisely retrace her steps.[171] Reasoning that there was "no virtual certainty that [the officer]'s review was limited to the photographs from [the girlfriend]'s earlier search,"[172] the court upheld the suppression of the child pornography evidence.[173] Under the private search doctrine, it is not clear what reasonable expectation of privacy Lichtenberger still had in this situation.

Natural adrenaline, panic, and confusion undoubtedly follows the discovery of criminal activity on a loved one's computer (not to mention the natural paranoia—"what if they think this is mine?"). It seems unreasonable to expect the private party to meticulously recreate the steps they took before and after the discovery of potentially earth-shaking facts such as those in *Lichtenberger*. In the end, such an approach will render the private search doctrine meaningless in the digital context, as officers will be unwilling to risk the frustration of their investigation that is sure to follow if the informant makes a slight misstep. Alternatively, police would only be further encouraged to conduct investigations with a wink and a nod, suggesting to private searchers "of course, these are *precisely* the images you looked at before and the *only* images you looked at before"—hardly a desirable result.

The first step of the *Jacobsen* analysis is to determine the scope of the private search and whether the government agent exceeded that scope in a subsequent search. If the government agent *has* exceeded the scope of the private search the court should then determine whether there was any remaining reasonable expectation of privacy. Not only did the court in *Lichtenberger* define the container too narrowly, but it also analyzed the remaining expectation of privacy too restrictively. By limiting "virtual certainty" to the images actually viewed by the private searcher, the Sixth Circuit ignored the statements of private searchers and law enforcement's expertise.[174]

Strikingly, the Sixth Circuit cited *United States v. Bowers* as support for a "near-certainty" standard regarding what law enforcement might find in expanding on a private search.[175] There, a private searcher located what appeared to be child pornography in a photo album.[176] The police searched the album and arrested the owner.[177] However, it is not clear that the private searcher and the police viewed the same

171. *Id.*

172. *Id.* at 488.

173. *Id.* at 491.

174. *See* United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001). *See also* United States v. Jacobsen, 466 U.S. 109 (1984) (demonstrating the reduced privacy expectation resulting from circumstances surrounding the government search).

175. *Lichtenberger*, 786 F.3d at 486. *See* United States v. Bowers, 594 F.3d 522, 524–26 (6th Cir. 2010).

176. *Bowers*, 594 F.3d at 524–25.

177. *Id.*

images.[178] While the Sixth Circuit was correct to point out the substantially increased privacy interests involved in digital storage, its approach to the problem is ultimately unworkable. Based on the *Lichtenberger* reasoning, the evidence from *Bowers* should also have been suppressed, as there was no indication that the police had viewed only the images viewed by the private searcher. The police could not have substantial certainty, therefore, that they would learn something not already learned in the private search. The Sixth Circuit's reasoning would nullify the private search exception with respect to both physical and digital containers. Alternatively, such reasoning would require a case-by-case approach where the scope of the private search was entirely dependent on the size and nature of the container involved. This approach seems to be at odds with the Supreme Court's refusal to distinguish "between 'worthy' and 'unworthy' containers" with respect to legitimate privacy interests.[179]

IV. Recommendation and Objections

A. *"Just Right"*

The Supreme Court has acknowledged the ongoing question of how best to limit "this power of technology to shrink the realm of guaranteed privacy."[180] This Note has acknowledged that the "traditional" approach is too broad. Viewing the entire digital storage device as a single container exposes too much of an individual's potentially private information and is inadequate to protect the individual's legitimate privacy interests. On the other hand, this Note has argued that the growing trend to treat the individual file as the container is too narrow. Such a narrow reading essentially extinguishes the private search doctrine in the not uncommon situation where a private party discovers incriminating data on a computer and the police need to verify the evidence before taking further action.

This Note urges courts to adopt a middle way—the "just right"—and begin their analysis of warrantless searches subsequent to a private search by defining the container "as the virtual file first opened by the private party." Then, courts should consider all the facts surrounding the government action to determine whether the officer's subsequent acts violated the owner's reasonable, legitimate privacy interest. As indicated by the "reasonable expectation of privacy" test for Fourth Amendment searches, this will be a fact intensive analysis, without convenient bright-line rules. The virtual folder method analogizes well with physical searches, provides law enforcement with a

178. *See id.* at 524–26.

179. California v. Greenwood, 486 U.S. 35, 47–48 (1988) (quoting United States v. Ross, 456 U.S. 798, 822 (1982)).

180. Kyllo v. United States, 533 U.S. 27, 34 (2001).

fairly predictable standard to guide them, and balances the legitimate aims of government against the individual interest in privacy.

We may be hard-pressed to say that a private search of part of a large digital storage device renders any of its other contents obvious or exposes them to "plain view." The *Lichtenberger* court was accurate in this respect. However, the Sixth Circuit's reasoning was flawed for two reasons. First, the court's application of a very narrow version of the container doctrine represents an all-or-nothing, black-and-white approach to the private search exception and container concept. Second, even assuming *arguendo* that the individual file was an appropriate container, the *Lichtenberger* court ignored the fact that the obvious character of the device's contents is not the only factor that may destroy a reasonable expectation of privacy in such contents.[181]

Compared to physical containers, it is more difficult to determine anything about the contents of a digital folder simply by opening the folder. By their very nature, their contents are often opaque to observation until a file is opened (although the use of "thumbnails" may provide more information about pictures in particular). This Note argues that the partitioned nature of data files in a computer is a circumstance that should be considered when determining the scope of a private search. The literal ability of the police to see all the contents of a container, however, is not the only ground that could support substantial certainty. This opacity in the digital realm makes "substantial certainty" about other files more difficult, but not impossible.

Because people typically store their data grouped in file folders, they indirectly create a different expectation of privacy in those files stored together. Computer users could choose to store their data together in a single large folder, or on the desktop. Most people, however, do not store their data this way. The reality is that people typically store similar items together, much as they do with physical items. Being stored in close proximity is not sufficient to give searches "substantial certainty,"[182] but the use of folders in the digital world that is very similar to the physical world reinforces that the container doctrine is still apt with respect to digital storage. In both cases, there is an understanding that by storing items together, you link access to these items. If one stores all one's jewelry in a box, then there is a reasonable expectation that another person who accesses the box will effectively access all of the jewelry, not just particular pieces they physically touch or see.

We should not change the nature of our Fourth Amendment analysis simply because the subject of a search is a digital storage device.[183] Delineating the scope of a private search at the file folder level seems

181. *See supra* Section II.A.2.

182. *See* United States v. Kinney, 953 F.2d 863, 866 (4th Cir. 1992).

183. Clancy, *supra* note 158, at 195–96.

a reasonable place to draw the line and it balances the public interest in law enforcement against the individual privacy interest. Of course, a judge may *ex post* determine that the size of the folder was so large that the owner retained some legitimate privacy interest in the data within that folder. The same could apply to a large physical container; a court could reasonably hold that the private search doctrine does not completely justify a warrantless search. And officers must exercise care by obtaining a warrant as soon as they reasonably can, in order to prevent further warrantless invasion of privacy.

B. *Objections*

Challenges are expected to this middle-ground approach. While the virtual folder method may have its own shortcomings, it is the approach that best considers both private and public interests.

1. This Approach is too Fact-Intensive and Will Muddy the Waters for Law Enforcement

Opponents may argue that this Note's emphasis on the particular circumstances surrounding a subsequent search would lead to uncertainty in police searches. The Supreme Court's avowed preference for categorical rules to guide law enforcement gives weight to this position.[184] Analysis that considers the totality of the circumstances could prove murky for law enforcement. However, the Court has also affirmed that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[185] The Fourth Amendment protects against "unreasonable" searches and seizures. Consequently, where a private search has destroyed a reasonable expectation of privacy, a government search is inherently reasonable; in fact, it is not a *search* at all, to the extent it does not exceed the scope of the private search. Any inquiry so focused on "reasonableness" will necessarily be fact-intensive. Indeed, it may be that the Fourth Amendment is resistant to general, bright-line rules by its very nature, at least with respect to anything but the broadest strokes.[186] The nearly limitless possible combinations of circumstances practically demand case-by-case analysis.[187] If a "search" is initiated by surveillance of a glass-walled public telephone booth,[188] but not of an open field on private property,[189] it stands to reason that applying the private search doctrine will require

184. Riley v. California, 134 S. Ct. 2473, 2491 (2014).
185. *Id.* at 2482 (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).
186. Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1197–2000 (1998) (describing the Fourth Amendment as a "spontaneous system" akin to the common law, amenable to gradual, incremental change, but not to a rigorous analytical breakdown).
187. *See id.* at 1198–99.
188. *See* Katz v. United States, 389 U.S. 347 (1967).
189. *See* Oliver v. United States, 466 U.S. 170 (1984).

a deeper analysis than simply tabbing a digital file as a "container" and excluding any search that fails to recreate the prior private search.

Some might accuse this Note's "reasonableness" aspect of being as dangerous to the container doctrine as the *Lichtenberger* decision. Because the ultimate basis for Fourth Amendment questions is "reasonableness,"[190] an argument could be made that the container doctrine is inapt in the digital context. While some may advocate for a return to fundamental Fourth Amendment principles,[191] this Note does not propose anything so drastic as dispensing with current jurisprudence on the private search exception. This Note instead advocates a middle ground that harmonizes both principle (balancing competing Fourth Amendment interests) and practice (the traditional container doctrine) while leaving modern courts flexibility to adjust to particular circumstances in their evidentiary rulings.

Guidelines under the Fourth Amendment should facilitate, not hinder, law enforcement in performing their duties.[192] Therefore, although categorical rules may be preferred, they should not carry the day if they create confusion or doubt for law enforcement, or otherwise tie their hands in carrying out legitimate police interests.

The private search doctrine would not be the first exception to the Fourth Amendment's resistance to bright-line rules. Considering the "open field" exception, the Supreme Court adopted a factor test—considering all the relevant circumstances—for "extent-of-curtilage-questions" rather than develop a categorical formula to determine the boundary between a landowner's "open field" and his "home" for Fourth Amendment purposes.[193] The Court "decline[d] the Government's invitation to adopt a 'bright-line rule.'"[194] Simply put, some applications of the Fourth Amendment are ruled by "common sense and ordinary human experience" rather than bright-line rules.[195]

The Supreme Court has consistently held that police searches are presumptively unreasonable unless sanctioned by a warrant issued by a magistrate, based on probable cause, and in consideration of the totality of the circumstances.[196] This warrant, and the probable cause on which it is based, limit the scope of a warranted search. Thus all of

190. Riley v. California, 134 S. Ct. 2473, 2482 (2014) (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).

191. *See* California v. Acevedo, 500 U.S. 565, 583 (1991) (Scalia, J., concurring).

192. *Riley*, 134 S. Ct. at 2491–92 (emphasizing the importance of clear guidance to law enforcement). *See also Oliver*, 466 U.S. at 181 (declining to analyze the "open field" doctrine on a case-by-case basis on the grounds that "police officers would have to guess before every search" whether their acts would fall under the Fourth Amendment).

193. United States v. Dunn, 480 U.S. 294, 301 (1987).

194. *Id.* at 301, n.4.

195. *See* United States v. Sharpe, 470 U.S. 675, 685 (1985) (discussing duration of *Terry* stops).

196. Florida v. Harris, 133 S. Ct. 1050, 1055–56 (2013) (citing Illinois v. Gates, 462 U.S. 213 (1983)).

the circumstances relating to the search must be considered in setting its scope. In the context of a private search, determining the appropriate scope similarly limits the law enforcement search.[197] It seems only appropriate to similarly consider all the circumstances surrounding a search to determine its lawful scope. This Note's approach does so by selecting a "just right" middle ground to start the analysis (thus providing clear guidance to law enforcement recreating private searches). Then, the court may *post hoc* examine the circumstances surrounding the search. It may be that the file folder involved was so large that the container doctrine could not reasonably be applied. Alternatively, there may be indicators such as folder title, file titles, or other circumstances that would create virtual certainty of the contents of *other* file folders than those opened by the private searcher.

2. This Approach Ignores the Literal Reality of Digital Storage

One of the obvious challenges for courts is sorting out the best way to conceptualize hard drives in the context of the Fourth Amendment.[198] This challenge is exacerbated by the fact that the literal reality of a hard drive does not match up with the virtual reality of a computer display.[199] Particularly in terms of the private search exception, courts must determine whether to aim for a concept of the digital storage that closely matches the reality of the device, or one that reflects the reality of the virtual display that officers and judges will be forced to deal with. By attempting to restrict the overbroad approach of *Runyan*, this Note's approach, while not closely matching the digital storage reality, best safeguards the competing aims of Fourth Amendment jurisprudence—individual privacy and law enforcement aims.

Judges are well-advised against delving too deeply into subjects on which they are not experts.[200] In *Crist*, for example, it seems fair to wonder if the court had a full understanding of how hard drives work when it attempted to divide a hard drive in a way at odds with the reality of data storage—the result of which was an unworkable and ultimately inconsequential rule.[201] In that vein, shouldn't the rules or guidelines established for Fourth Amendment jurisprudence be accessible to judges and attorneys who will try such matters, and make sense to lay police officers who must work under such rules? This Note's proposition is a more restrictive conceptualization of digital

197. *See supra* Section II.A.1.

198. *See generally* Palumbo, *supra* note 116 (noting the challenges of various conceptualizations).

199. *See id.* at 988–89.

200. MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 958 (2005) (noting that "[j]udges have no specialized technical ability to answer questions about present or future technological feasibility").

201. *See* Palumbo, *supra* note 116, at 997–98. *See also* United States v. Crist, 627 F. Supp. 2d 575, 586 (M.D. Pa. 2008).

containers, better protecting individual privacy than the broad "traditional" approach. However, the common-sense nature of the virtual file conceptualization serves the legitimate ends of law enforcement far better than stricter approaches which unreasonably hamper the police.

It is beyond the scope of this Note to fully analyze the technical operation of digital storage devices. Some have argued that the realities of digital storage are so drastically different from physical searches and seizures that we cannot draw a fair analogy.[202] However, as digital security measures continue to develop alongside digital storage, that may not be the case. Passwords can function as locked doors, partitioning as separate rooms, and encryption as further security. In many ways digital storage becomes more analogous to physical space as technology develops, particularly with respect to the virtual display accessed by the user. If this is the case, then our traditional concepts of Fourth Amendment doctrines may in fact serve us well in the digital world.

The court in *Crist*, along with commentators make a great deal about the complexity of the literal process underlying the visual display of a digital device.[203] Under a warranted search, where law enforcement might conduct a full forensic analysis of the digital storage device, this distinction is more relevant. Under a warrant authorizing a search for a particular type of data, for instance, it is conceivable that police would exceed the scope of the warrant by creating a "hash value" of portions of the hard drive where they had no reason to think evidence of a crime was stored. However, under any but the laxest standard for the private search exception—or unless the private party conducted his or her own forensic analysis—such a detailed search of a digital device would exceed the scope of the private search. Therefore, the distinction of the literal reality of the digital storage and the virtual display is less urgent with respect to the private search exception.

If a method fairly analogizes the digital storage universe in lay terms without unreasonably infringing privacy interests, should we ignore such an analogy based solely on the fact that it is not strictly accurate in terms of the opaque mechanical processes of modern technology? The over-emphasis of arcane minutiae ignores the practical realities of law enforcement "on the ground." Private citizens may often be flustered by the discovery of criminal data on a friend or loved one's computer. It hardly seems reasonable to demand that they be able to exactly recreate their search in order to satisfy the technophile's conception of what most closely replicates the unseen reality of modern hard-drive technology.

202. *See, e.g.*, Kerr, *supra* note *66, at 533.*
203. *See id.*; *see also Crist*, 627 F. Supp. 2d at 584–87.

Courts and scholars alike have noted the challenges of conceptualizing containers in the digital world, some going so far as advocating abrogation of the principle altogether with respect to digital searches.[204] Without a doubt, the challenges are well-noted. However, completely abandoning the container concept would effectively nullify the private search doctrine. Without some conceptualization of the container doctrine, law enforcement would only be able to review the precise files searched by the private party. As *Lichtenberger* demonstrates, the result of this approach is harsh. What this Note attempts to do is to identify workable parameters for containers in the digital world while staying true to the principles underpinning the Fourth Amendment.

While it is true that digital storage amounts to a dramatically *larger* type of storage than a physical container, it is not clear that it therefore amounts to an entirely different *type* of thing. In both the physical and the digital world, citizens may secret away things they would rather not have public, thus creating a reasonable expectation of privacy for purposes of the Fourth Amendment. In both cases that expectation of privacy may be frustrated by the fact of another private individual's snooping. In the physical world, accessing a closed container frustrates the owner's privacy interest in the contents of the container, not because the private party looks at each and every item, but because by placing those items together in a closed container, the owner has essentially linked his or her expectation of privacy in each item together. So, for instance, if a private party opened another's foot locker and saw a severed head laying on top of other objects and immediately ran to call the police, the police would most likely be permitted to take more time and review the contents of the locker more thoroughly. By grouping things together for storage, the owner reasonably must expect that someone able to see one thing would also be able to see the other things stored with it. The scope of the private search, seen this way, has more to do with what the private party *could* have seen, rather than identifying what the party, in fact, *saw*. This principle applies as well to the digital world as to the physical.

What then to do about containers within containers? With the exception of identical packages within the same container, where the

204. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (stating that reliance on container analogies may "oversimplify a complex area of Fourth Amendment doctrines"); Palumbo, *supra* note 116, at 980 (positing that characterization of hard drives as containers is not viable); Benjamin Holley, Note, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 702 (2010) (calling the container analysis "entirely unpersuasive in the virtual realm"); Clancy, *supra* note 158, at 202–03 (2005) (noting concerns about applicability of the container doctrine in the digital world); *Crist*, 627 F. Supp. 2d at 586 (rejecting the argument that a computer is analogous to a container); United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (focusing only on the "virtual certainty" of the officer and effectively ignoring the container concepts).

identity of one opened package "spoke volumes" about the remaining packages,[205] there appears to be agreement that a private search of a container does not *per se* frustrate the reasonable expectation of privacy of containers therein.[206] In principle, this concept is related to the fact that the steps one takes to maintain privacy are related to what reasonable expectation of privacy one has,[207] and serves to limit the otherwise broad scope of the container doctrine. Each container represents a distinct attempt to take precautions against prying eyes, and therefore suggests a fresh expectation of privacy, which is not defeated by opening the larger container.

This Note's recommendation that courts use the virtual file folder as a container meshes well with this view of containers generally. By searching and turning over a laptop to the police, a private search has severely compromised the owner's expectation of privacy in the laptop's contents. However, various virtual layers of protection within the digital world limit the exposure of vast amounts of private data. Although the real-world mechanism of digital storage makes a physical container approach unworkable,[208] data owners do make choices about grouping data together that closely resemble physical reality.

Relatedly, as technology advances further, it may be that the digital world will continue to resemble the physical world more and more. Most operating systems are premised on groupings of folders.[209] There are "how-to" articles laying out the most efficient way to arrange files into various folders[210] and studies on the various ways subjects use digital file folders.[211] In fact, despite the very different ways in which they operate, digital storage devices are functionally very similar to physical containers. Technically, a hard drive disk is "magnetic recording material . . . layered onto a high-precision aluminum or glass disk . . . then polished to mirror-type smoothness."[212] In prac-

205. United States v. Bowman, 907 F.2d 63, 65 (8th Cir. 1990) (quoting United States v. Jacobsen, 466 U.S. 109, 121 (1984)).

206. *See* United States v. Kinney, 953 F.2d 863, 866 (4th Cir. 1992) (holding that police exceeded the scope of a private search of a closet when they opened a bag—which the private party had not searched—inside the closet); United States v. Donnes, 947 F.2d 1430, 1436 (10th Cir. 1991) (holding that opening a camera lens case within a glove searched by a private party constituted a new search).

207. *See, e.g.*, Florida v. Riley, 488 U.S 445, 454 (1989) (O'Connor, J., concurring) ("If they do not take . . . precautions, they cannot reasonably expect privacy.").

208. *See* discussion *supra* Section II.B.

209. *Computer File*, WIKIPEDIA, THE FREE ENCYCLOPEDIA, https://en.wikipedia.org/wiki/Computer_file (last visited Feb. 29, 2016) [https://perma.cc/3KVB-6SBR].

210. *See* K.J. McCorry, *How to Organize Computer Documents*, OFFICIENCY, http://computerorganizing.com/ [https://perma.cc/7YME-4B4Z].

211. *See* Christopher S.G. Khoo et al., *How Users Organize Electronic Files on Their Workstations in the Office Environment: A Preliminary Study of Personal Information Organization Behavior*, 11 INFO. RES. (2007), http://www.informationr.net/ir/12-2/paper293.html [https://perma.cc/8YKW-4AFS].

212. Brain, *supra* note 113.

tice, "a computer is a container of containers of documents."[213] Much as they do in the physical world, individuals tend to group items or information together in containers.

By storing digital data in folders, individuals manifest a linked expectation of privacy, similar to that manifested in physical containers.[214] It is reasonable, therefore, to treat data stored in a container as being in "plain view" once a private searcher has opened that container.[215] How to best apply the container doctrine in the digital realm is a more appropriate question than whether the container doctrine is applicable to digital storage at all.

Other aspects of digital storage—such as passwords, hidden files, and encryption—provide very reasonable analogies to locked doors, walls, physical containers, and other real-world security measures. In the virtual world now, it is increasingly true, as in the physical world, "[i]ndividuals who seek privacy can take precautions . . . to avoid disclosing private activities to those who pass by."[216] And as such, courts are more entitled to argue that "If they do not take such precautions, they cannot reasonably expect privacy from public observation."[217]

A file folder standard for containers harmonizes with the principle that a private intrusion should not open the door to a general search,[218] while giving police the practical flexibility they need to gather evidence. The traditional container view would admittedly allow the former, while the suggested strict approach would frustrate the latter, and prevent law enforcement from making use of information "freely made available."[219]

The Supreme Court has wrestled with the changing face of technology for much of the twentieth and twenty-first centuries.[220] It has used these challenges to refine Fourth Amendment jurisprudence in light of the fundamental goal of protecting privacy while enabling the state to preserve the security of the people. The approach of the Sixth Circuit in *Lichtenberger* represents in practice a wholesale change rather than a refinement.

---

213. Clancy, *supra* note 158.

214. *See supra* Section II.A.1.

215. *See id.*

216. *See* Florida v. Riley, 488 U.S. 445, 454 (1989) (O'Connor, J., concurring).

217. *Id.*

218. *See* Walter v. United States, 447 U.S. 649, 657 (1980).

219. United States v. Harling, No. 2:13-cr-96-FtM-38CM, 2014 U.S. Dist. LEXIS 107398, at *9 (M.D. Fla. Aug. 4, 2014).

220. *See* Kyllo v. United States, 533 U.S. 27 (2001) (thermal-imaging technology); Katz v. United States, 389 U.S. 347 (1967) (telephone bug). *See also* Florida v. Riley, 488 U.S. 445 (1989) (helicopter); California v. Ciraolo, 476 U.S. 207 (1986) (fixed-wing aircraft); United States v. White, 401 U.S. 745 (1971) (recording device).

3. This Approach Overstates the Fallout from *Lichtenberger*

Opponents may argue that this Note goes too far in claiming that *Lichtenberger* would completely nullify the private search doctrine with respect to digital storage. But the realities of obtaining a warrant demonstrate this, particularly with respect to "possession" charges, such as possession of child pornography. To be sure, obtaining a warrant as early as possible is the best option for law enforcement. However, as an initial matter, officers must make a judgment call on what evidence they will need to obtain a warrant to search further. Commonly, the officer will need to observe the evidence of criminal activity him- or herself.[221] Once there is evidence sufficient for a warrant, the officer would be wise to discontinue recreating a private search. However, the Sixth Circuit will necessarily place officers in a position of having received a report of criminal possession, unable to obtain a warrant without first viewing the alleged material, but at risk of losing the case if the private party who initiated the search makes an error in recollection.

For instance, suppose slightly different facts for the *Donnes* case. Rather than a glove with a syringe and lens case in it, suppose that the private party had discovered a glove with *two* lens cases in it. The private party then opens one lens case and discovers apparent contraband. The private party leaves the glove for a moment and contacts a police officer to come to the scene. Once there, the police officer asks the private party to show him what he found. By mistake, the private party opens up the wrong lens case. Under the *Lichtenberger* reasoning, the evidence of contraband in the first lens case would be suppressed and the owner would go free because of an error in the recollection of the private party—ironically just the sort of thing that the Supreme Court has used to *justify* the private search doctrine.[222]

V. Conclusion

Modern technology allows individuals to gather unprecedented amounts of data together in one place. Data a person fifty years ago would have kept in a box, or filing cabinet, or even a library, now fits in a block the size of a legal textbook. This level of storage creates a constitutional "too hot" scenario under the Goldilocks Principle. If courts conceptualize a storage device as a single closed "container" under the Fourth Amendment, the owner's privacy expectation in the entire device would be frustrated by a third party viewing any part of it. Police could conceivably use the private search exception to gain access to unthinkable amounts of private information. If courts con-

221. *What Is a Search Warrant and What Does It Take to Get One?*, Search and Seizure FAQ, NOLO, http://www.nolo.com/legal-encyclopedia/search-seizure-faq-29092-3.html [https://perma.cc/34SS-NR72].

222. United States v. Jacobsen, 466 U.S. 109, 119 (1984).

ceptualize individual files as distinct containers, conversely, an unacceptable "too cold" scenario arises. Law enforcement could only view the identical files viewed by a private searcher, or risk exclusion of the evidence. The private search exception would be effectively annihilated in the digital world just as digital storage of incriminating evidence has become the norm. Much like Goldilocks, we must find a "just right" conceptualization.

This Note's "just right" approach would treat each virtual folder as a container for Fourth Amendment purposes. This conceptualization remains true to the heart of the Fourth Amendment and the private search exception. By allowing courts flexibility in setting the scope of the private search, this conceptualization is consistent with the "reasonableness" standard that underlies the Fourth Amendment. Additionally, this middle ground is consistent with the traditional private search exception rationale. Police should not be effectively forced to avert their eyes from evidence brought by a third party, as would happen under the strict "too cold" conceptualization. Neither should the police conduct a sweeping general search, however, as is risked by the broad "too hot" conceptualization. Finally, the "just right" approach appropriately balances the government's law enforcement interests against individual privacy interests. The increased data storage of digital devices weighs heavily for privacy interests in this balance. The everyday use of file folders to organize and store data on the virtual desktop, however, has altered the typical expectation of privacy in data files within the same folder. This is similar to linking privacy expectations in multiple items stored in a single container.