DEFINING THE LIMITS OF THE PRIVATE-SEARCH DOCTRINE IN AN EXPANDING DIGITAL LANDSCAPE

*Kendall Van Ameyde**

INTRODUCTION

Computers, cell phones, and other transformative technologies conveniently hold for numerous Americans "the privacies of life."[1] With the increasing storage capacities, and the reductions in the physical size of technologies today,[2] a complete picture of an individual's life is easily reconstructed through the vast amounts of information stored on a computer or cell phone,[3] including bank statements, addresses, photographs, and browsing history.[4]

* Executive Editor, *Michigan State Law Review*; J.D. 2017, Michigan State University College of Law; B.S. in Political Science, Grand Valley State University. The author would like to thank Professor Barbara O'Brien for her guidance during the writing process. The author would also like to thank Marie Rauschenberger and Elizabeth Kingston for their encouragement and support during the writing process. Finally, the author would like to thank her parents, Jan and Lee, for their love and support.

1 Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

2 *See Computers & the Internet*, FUTURETIMELINE.NET (2011), http://futuretimeline.net/subject/computers-internet.htm#data-storage. Data storage has increased at exponential rates in just fifty years and will continue to grow. *Id.* In 1956, IBM launched the first computer weighing over a ton with a total storage capacity of 4.4MB. *Id.* By 2010, home computers had storage capacities of one terabyte. *Id.*

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

4 *See Riley*, 134 S. Ct. at 2489.

First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

The technology becomes a "virtual diary"[5] of an individual American citizen ready to be willfully explored or unwillingly examined. With increasing storage capabilities of technology, especially computers, the resulting implications for a citizen's constitutional privacy rights will be extremely hard to safeguard from overzealous government intrusion.[6]

With these advances in technology, there is a dark side to its use, including the ease with which criminals can carry out illegal activities, such as hacking or releasing a computer virus, or hide other offenses, including storage of evidence of child pornography on a computer.[7] The fact that most cases involving computers have dealt almost exclusively with criminal conduct should "not serve as a bar to the development of Fourth Amendment doctrine that properly balances the privacy concerns of individuals against the needs of law enforcement officials moving forward."[8] Thus, any American citizen who stores important data on a computer today could be the one at risk of government intrusion tomorrow.[9]

This worrisome government intrusion is highlighted by one of the many established warrant exceptions under the Fourth Amendment, the private-search doctrine.[10] Under the private-search doctrine, private parties acting on their own are not

---

5 Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) (stating that "computers are playing an ever greater role in daily life and are recording a growing proportion of it. In the 1980s, computers were used primarily as glorified typewriters. Today they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

6 *See infra* Subsection III.A.1.

7 *See* Corey J. Mantei, *Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches*, 53 ARIZ. L. REV. 985, 987–88 (2011).

8 Marc Palumbo, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 980 (2009).

9 *See id.* at 979–80.

It is difficult for any judge to craft a rule that excludes evidence of such despicable acts when the government has a seemingly rational justification for carrying out the search in the manner it does. These vulnerabilities, however, do not only impact child pornographers. Given the increasing technological changes surrounding hard drives and data storage, the child pornographer defendant of today may very well turn into the business executive defendant of tomorrow. Businesses that store massive amounts of sensitive material on central servers or databases are at risk. Professionals who conduct sensitive operations and communicate via e-mail are at risk. In fact, anyone who stores important data on a computer is at risk.

10 *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (showing that the Fourth Amendment does not apply to the actions and searches of private individuals).

subject to regulation by the Fourth Amendment; therefore, if a private party conducts a search without participation of law enforcement, then the private party may show police what was found during the private search regardless of whether law enforcement would have been able to initiate a search in the first place.[11] However, if law enforcement searches for information that is beyond the scope of the private party's search, then the Fourth Amendment, which includes the individual's privacy, is violated.[12]

An issue then arises: "When a private party sees a file on a computer, what exactly has been searched for purposes of later reconstruction?"[13] The private party can either show police (1) the exact file or folder the private party saw or (2) everything located in the whole computer.[14] The Sixth Circuit recently examined this question of how the private-search doctrine extends to computers in *United States v. Lichtenberger*,[15] creating a circuit split concerning the proper application of the private-search doctrine to data stored on a personal computer.[16] The Sixth Circuit suppressed all of the evidence obtained as the product of an unconstitutional search and applied a virtual file-or-folder-level approach to the private-search doctrine for information discovered by a private party.[17] This approach involves searching computers for only the information contained in a single file or folder rather than searching everything located in the whole computer, which could lead to intrusive and alarming results.[18]

---

11 *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (stating that the Court has consistently interpreted protection from unreasonable searches and seizures "as proscribing only governmental action" and that it is not applicable "'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official'") (quoting Walter v. United States, 447 U.S. 649, 662 (1980)).

12 *See* Orin Kerr, *Sixth Circuit Creates Circuit Split on Private-Search Doctrine for Computers*, WASH. POST: THE 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/.

13 *See id.*

14 *See id.*

15 *Lichtenberger*, 786 F.3d at 479–80.

16 *See* Kerr, *supra* note 12.

17 *See Lichtenberger*, 786 F.3d at 485–86.

18 *See id.* at 490–91. "In light of the information available at the time the search was conducted, the strong privacy interests at stake, and the absence of a threat to government interests, we conclude that Officer Huston's warrantless

In contrast, the Fifth and Seventh Circuits have considered the entire computer to be within the scope of a private search.[19] This approach leaves the whole container open to exhaustive search by the government after a private party has viewed only a single discrete file.[20] "A computer is like a container that stores thousands of individual containers in the form of discrete files."[21] Unfortunately, this approach is not an attempt to be more thorough; it is akin to a fishing expedition.[22] The vast difference in scope between searching one file or folder versus a whole computer full of data and endless private information is too extreme to be ignored.[23]

Advancing technologies, including police surveillance technologies, along with the application of the private-search doctrine, raise serious privacy concerns for individuals.[24] The virtual file-or-folder-level approach, and the whole-computer

---

review of Lichtenberger's laptop exceeded the scope of the private search Holmes had conducted earlier that day, and therefore violated Lichtenberger's Fourth Amendment rights to be free from an unreasonable search and seizure. The laptop evidence and evidence obtained pursuant to the warrant issued on the basis of its contents must be suppressed." *Id.* *See also* Kerr, *supra* note 5, at 556.

19 *See* Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012) (stating "per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches. Because S.R. and her mother knew the contents of the digital media devices when they delivered them to the police, the police were 'substantially certain' the devices contained child pornography"); United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001) (holding that "the police in the instant case did not exceed the scope of the private search if they examined more files on the privately-searched disks than Judith and Brandie had").

20 *See* Kerr, *supra* note 5, at 555.

21 *Id.*

22 *See* Benjamin Holley, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 703 (2010) ("The difference in scope undermines the spirit and intent of the private search exception. Such an act is not merely examining the computer 'more thoroughly,' but is instead fishing in entirely uncharted waters.").

23 *See id.*

24 *See* Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1132–33 (2011) ("Technological developments have also reshaped police surveillance techniques and created major doctrinal difficulties for courts in applying the Fourth Amendment. At the founding of the nation, police and other governmental agents did not have sophisticated spying and surveillance technologies at their disposal. Governmental agents might have tried to eavesdrop on their fellow citizens in taverns or other public settings, and might even have tried to listen outside of a suspect's window. However, without technology, the opportunities for successful eavesdropping were more limited. Today, eavesdropping and other surveillance technologies have gone high tech and created Orwellian possibilities for snooping.").

approach, are the two approaches courts currently apply in order to solve this conflict with computer evidence and the Fourth Amendment's regulation of the process, but there is no uniform, or clear approach.[25] However, the narrow application of the private-search doctrine is best achieved by the virtual file-or-folder-level approach, as opposed to the whole-computer approach, which can have devastating results for individual privacy, and liberty,[26] because computers are akin to homes that are historically protected from government intrusion.[27]

Government should be restrained in how much it can search personal computers, cell phones, and other technology without a warrant after a private citizen finds evidence of crime on a computer and calls for help because the idea of limited government forms the basis of the Fourth Amendment.[28] Therefore, the Sixth Circuit's data-based approach, or virtual file-or-folder-level approach,[29] is more reasonable[30] because a search conducted "in violation of the Constitution is not made lawful by what it brings to light."[31] Until this issue reaches the Supreme Court for clarification, the best way to address the narrow application of the private-search doctrine is to apply the virtual file-or-folder-level approach, and to take more protective measures on a state level, such as creating specific guidelines and police procedures as well as amending state constitutions to be more protective of privacy.[32]

Part I of this Note outlines the origins and legal history of the Fourth Amendment, and describes the current protective measures states are instituting regarding the search and seizure of digital evidence. Part II discusses the legal history and application of the private-search doctrine to technology—specifically computers—and analyzes the differing approaches courts have taken to determine the appropriate zone of a private search. This zone can include a virtual file-or-folder-level approach or can be based on the whole computer. Part III

---

25 *See infra* Sections II.B-C.

26 *See infra* Part III.

27 *See* Kerr, *supra* note 5, at 533 ("Computers are like containers in a physical sense, homes in a virtual sense, and vast warehouses in an informational sense.").

28 *See* Kerr, *supra* note 12.

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

30 *See infra* Part III.

31 Byars v. United States, 273 U.S. 28, 29 (1927).

32 *See infra* Section I.B.

advocates for a narrow application of the private-search doctrine in the context of modern technology to better preserve individual privacy, and to avoid an application of the private-search doctrine that is too broad to be effective and constitutional. Finally, Part III also asserts solutions to the application dilemma involving the private-search doctrine, including that states must adopt more protective measures for dealing with private-party searches of current technology, especially computers.

I. THE FOURTH AMENDMENT: LEGAL HISTORY AND CURRENT STATE APPLICATION

Searches and seizures have consistently implicated privacy interests throughout history. The King of England in the 1760s used general warrants in England and writs of assistance in colonial America, which allowed for unlimited government authority to search private homes and businesses.[33] These general warrants failed "to specify the place or persons to be searched or the things or persons to be seized, thus permitting random or blanket intrusion into the private affairs of the people at the discretion of the police."[34] Use of writs of assistance, or general warrants were one of the grievances that led to the American Revolution.[35] Framers wanted to restrict the use of these warrants, so they crafted the Fourth Amendment[36] to limit government search authority.[37] The main principles that the Framers of the Constitution used to help lay the foundation for the Fourth Amendment were the belief in limited government power and discretion[38] and that privacy concerns and security

---

33 *See* Mantei, *supra* note 7, at 988–89.

34 EDWARD C. FISHER, SEARCH AND SEIZURE 3 (1970).

35 *See id.* at 4.

36 *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

37 *See* Mantei, *supra* note 7, at 989.

38 *See* Raymond Shih Ray Ku, *Modern Studies in Privacy Law: Searching for The Meaning Of Fourth Amendment Privacy After Kyllo v. United states: The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002)

> ([T]he amendment is best understood as a means of preserving the people's authority over government - the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens. The

concerns should be left mainly to "the people."[39]

Furthermore, the Supreme Court has attempted to clarify the meanings of the Fourth Amendment's terms "search" and "seizure" because they are not explicitly defined in the Amendment.[40] A "search" occurs when "first . . . a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, . . . the expectation [is] one that society is prepared to recognize as 'reasonable.'"[41] A "seizure" of property occurs when there is some meaningful interference with an individual's possessory interests in that property.[42] Even though the Fourth Amendment acts as a barrier to government intrusion, it serves only as a minimum standard for the application of the search-and-seizure requirement to the states.[43] States are free to have stronger and more specific protections through legislation, common law, and state constitutions.[44]

However, with the introduction and invention of new transformative technologies and the increased storage capacities of these technologies, a strong concern arises with the application of the private-search doctrine to computers.[45] The private-search doctrine is one of the exceptions to the Fourth Amendment's general warrant requirement[46] and allows a private party to simply show law enforcement what he found even though law enforcement lacks probable cause.[47] Private parties acting on their own initiative are not subject to the Fourth Amendment

---

amendment does so as part of the rich tapestry that is the Constitution, and cannot be viewed in isolation, but must at the very least be viewed together with the principles embodied in the constitutional separation of powers.).

39 U.S. CONST. pmbl.

40 *E.g.*, *Jacobsen*, 466 U.S. at 113.

41 Katz v. United States, 389 U.S. 347, 361 (1967).

42 *See Jacobsen*, 466 U.S. at 113.

43 *See* Hanni Fakhoury & Nadia Kayyali, *Know Your Rights!*, ELEC. FRONTIER FOUND. (Oct. 2014), https://www.eff.org/issues/know-your-rights.

44 *See infra* Section I.B.

45 *See* Kerr, *supra* note 5, at 532–34.

46 *See* 68 AM. JUR. 2D *Searches and Seizures* § 114 (Exceptions to the warrant requirement include searches and seizures conducted incident to a lawful arrest, those yielding contraband in plain view, those in the hot pursuit of a fleeing criminal, those limited to a stop and frisk based on reasonable suspicion of criminal activity, those based on probable cause in the presence of exigent circumstances, and those based on consent.).

47 *See Jacobsen*, 466 U.S. at 113.

warrant requirement; therefore, the party can show law enforcement what was discovered during the initial search.[48] Now, with the proliferation of laptop computers, desktop PC's, tablet computers, cell phones, and other technologies, a new "digital persona"[49] has been created, increasing the possible zones of privacy that are easily breached by anyone with access to a device.[50] The Supreme Court has started to examine the application of the Fourth Amendment to current technology, and states are working to resolve privacy issues implicated by instituting new procedures in police manuals, issuing new common-law decisions, and revising constitutions.[51] The Fourth Amendment has a long history, and it has established a few clear rules to guide the states in the application of search-and-seizure law.

A. Early Fourth Amendment Jurisprudence

Early Fourth Amendment jurisprudence sheds light on how the search-and-seizure requirements have transformed through case law, when a person has an expectation to privacy, and what course the Supreme Court is charting in applying the Fourth Amendment to new technology. Two of the earliest cases involving the Fourth Amendment and technology are *Olmstead v. United States*[52] and *Goldman v. United States*,[53] where the Court reasoned that searches should be limited to tangible property.[54] In *Olmstead*, police officers, acting without judicial approval, did

---

48 *See id.*

49 *Technology and Privacy: The New Landscape* (Philip E. Agre & Marc Rotenberg eds., 1997), http://polaris.gseis.ucla.edu/pagre/landscape.html.

50 *See id.*

51 *See infra* Section I.B.

52 Olmstead v. United States, 277 U.S. 438, 455 (1928).

53 Goldman v. United States, 316 U.S. 129, 135 (1942) (holding "that the use of the detectaphone by Government agents was not a violation of the Fourth Amendment").

54 *See id.* at 134–35. *See also Olmstead*, 277 U.S. at 466

> (Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure. We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.).

not violate defendants' Fourth Amendment rights by wiretapping the private telephone conversations of those defendants suspected of being involved in a bootlegging conspiracy.[55] The Fourth Amendment's protection of persons, houses, papers, and effects was not violated by law enforcement "accessing telephone lines from a public street"[56] because law enforcement did not access any of these specified protected places. Similarly, in *Goldman*, federal agents did not violate the Fourth Amendment when they placed a detectaphone against a partition of the wall office in order to listen to members of a conspiracy who held conversations in that office.[57] The Court eventually deviated from this property-based approach,[58] but even so, a computer can be considered a form of property, an "effect" in the words of the Fourth Amendment, subject to protection.[59]

The Court later considered the importance of technology and individual privacy concerns in *Katz v. United States* and effectively overruled *Olmstead* and *Goldman*.[60] Privacy was the main focus in the *Katz* decision rather than the traditional property-based approach, and the Court expanded the scope of the Fourth Amendment by setting forth a two-part test to determine whether a search occurred.[61] Using this test, a court examines whether an individual had a subjective expectation of privacy and whether that expectation was reasonable.[62] This test is now used to determine whether there has been a search under the Fourth Amendment.[63] In *Katz*, the Court held that the government violated the Fourth Amendment and defendant's

---

55 *See Olmstead*, 277 U.S. at 456–57, 469.

56 Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 81 (2012).

57 *See Goldman*, 316 U.S. at 134–35.

58 *See Katz*, 389 U.S. at 353.

59 *See* Kerr, *supra* note 5, at 538 ("Computer searches and home searches are similar in many ways. In both cases, the police attempt to find and retrieve useful information hidden inside a closed container.").

60 *See Katz*, 389 U.S. at 353 ("We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

61 *See id.* at 361 (explaining the twofold requirement: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

62 *See id.*

63 *See* PAUL J. LARKIN, JR., THE HERITAGE FOUND., THE FOURTH AMENDMENT AND NEW TECHNOLOGIES 4 (Sept. 19, 2013), http://thf_media.s3.amazonaws.com/2013/pdf/lm102(new).pdf.

privacy when it listened to and recorded defendant's conversations while using a public telephone booth.[64] The Court reasoned that "the Fourth Amendment protects people, not places" and stated that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[65] Therefore, an individual has a right to protect what he deems private, even if it is in an area or a container that is accessible to the public.[66] In *Katz*, the defendant sought to keep his telephone conversations private.[67]

While *Katz* expanded the Fourth Amendment's scope by focusing on an individual's reasonable expectation of privacy, the Court also brought back a property-based approach—the Trespass Test—in *United States v. Jones*.[68] In *Jones*, the Fourth Amendment was again applied to technology.[69] The Court held that the Government's use of a GPS device on an individual's vehicle, and its use of that technology to monitor the vehicle's movements, constituted a search.[70] The Court reasoned that it must apply "an 18th-century guarantee against unreasonable searches" in order to provide the minimum "degree of protection it afforded when it was adopted."[71] The government's placement of the GPS on the individual's vehicle—his personal effect—was a trespass and a search under the Fourth Amendment as the device monitored and tracked every individual movement for several weeks.[72] Following *Jones*, the current test utilized to determine

---

64 *See Katz*, 389 U.S. at 353.

65 *Id.* at 351, 359.

66 *See id.* at 351 (stating that "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

67 *See id.* at 351–52.

68 United States v. Jones, 132 S. Ct. 945, 952 (2012) (stating that "[t]he *Katz* reasonable-expectation-of-privacy test has been *added* to, not *substituted for*, the common-law trespassory test").

69 *Id.* at 949 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

70 *Id.*

71 *Id.* at 411.

72 *Id.* at 429–30.

> Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way. *Id.*

whether a search has occurred begins first by asking if there has been a trespass into an area enumerated under the Fourth Amendment ("persons, houses, papers and effects").[73] If there has been a trespass for the purposes of obtaining information, then a search has occurred.[74] Second, if there has been no trespass, then the reasonable-expectation-of-privacy test from *Katz* is used.[75]

These Fourth Amendment cases are vital to understanding the current debate over the private-search doctrine because they lay the foundations for what is considered an appropriate search, and what is a reasonable expectation of privacy.[76] Additionally, the cases demonstrate the evolution of Fourth Amendment search-and-seizure law and the importance placed on privacy.[77] The private-search doctrine as it relates to current technology is ripe for review by the Supreme Court, but until such a decision is made, states have attempted to address the serious privacy concerns raised in this new age of technology.[78]

B. State Protective Measures for Computer Searches and Digital Evidence

Due to the proliferation of new technology, states have

---

73 *Id.* at 405 ("Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.").

74 *See* Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 224–25 (2012). Writing for the Court, Justice Scalia finds that physical intrusion upon private property—a vehicle in this case—for the purpose of obtaining information constitutes a Fourth Amendment search. More surprisingly, Justice Scalia pointedly rejects *Katz* as applicable at all in this case. While he recognizes *Katz* as one authoritative standard in assessing the threshold question of whether a search has occurred, he believes that *Katz* never supplanted the basic trespass test from *Oldman*. Rather, "the *Katz* reasonable-expectation-of-privacy-test has been *added to*, not *substituted for*, the common-law trespassory test." In a case where the government intrudes upon a constitutionally enumerated area—an 'effect' in the case of *Jones*—the Court has no need to turn to *Katz*. *Id.*

75 *See id.*

76 *See Katz*, 389 U.S. at 350 ("That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion.").

77 *See id.*

78 *See Computer Crime Statutes*, NAT'L CONF. OF ST. LEGISLATURES (Dec. 5, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

attempted to address the changing nature of crime as it applies to computers. Every state has computer crime statutes targeting criminals who invade and attack another individual's computer and information,[79] but there are few statutes that protect individuals from law-enforcement intrusions, especially in instances where the private-search doctrine is invoked. Though some states have more protective search-and-seizure laws, these states are a minority, and even these enhanced protections may not properly protect an individual's privacy concerns in a computer.[80] Numerous states have created computer-crime task forces that actively work with prosecutors and state, county, and local law enforcement in order to train them about the legal issues involved with the investigation and the admissibility of digital evidence.[81] For instance, New Jersey has such a statewide focus on computer crime and has created a "Computer Evidence Search & Seizure Manual" in order to provide much-needed guidance to protect individuals' privacy and to allow law enforcement to properly conduct their jobs.[82] Similarly, the federal Office of Legal Education has attempted to provide guidance to states dealing with searches and seizures of computers and digital evidence.[83] This manual helps to define the current issues with search and seizure, including the private-search doctrine, and the proper limits to such a search.[84] Finally, some states have attempted to address these new search-and-seizure concerns by implementing procedures specifically targeting computer searches and digital evidence.[85]

While the Court has yet to determine the proper application of the private-search doctrine to modern technology, some states

---

79 *See id.*

80 *See* Monica R. Shah, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace*, 105 COLUM. L. REV. 250, 252 (2005).

81 *See Computer Evidence Search & Seizure Manual*, N.J. DEP'T OF LAW & PUB. SAFETY, DIVISION OF CRIMINAL JUSTICE 1–2 (Apr. 2000), http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

82 *See id.*

83 *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, OFF. OF LEGAL EDUC., EXEC. OFF. FOR U.S. ATT'YS ix–xii (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

84 *See id.* at 10–11.

85 *See Electronic Search Warrants 12.701*, CINCINNATI POLICE DEP'T PROC.MANUAL (Mar. 3, 2009), http://www.cincinnati-oh.gov/police/assets/File/Procedures/12701.pdf (showing Cincinnati revised its police manual to accommodate new technology and electronic search warrants).

have been proactive in enacting more protective provisions than the Fourth Amendment provides. Massachusetts was the first state to lead the charge in establishing protections against unreasonable searches and seizures and overzealous government intrusion in its constitution, and the Massachusetts's provision may have influenced the adoption of the Fourth Amendment found in the federal Bill of Rights.[86] States also have the ability to set their own protections through common law in addition to more protective state constitutions.[87] Connecticut's constitution is one example of a state measure that tends to be more protective of individual privacy than the Fourth Amendment.[88]

Under Connecticut's constitution:

The people shall be secure in their persons, houses, papers and possessions from unreasonable searches or seizures; and no warrant to search any place, or to seize any person or things, shall issue without describing them as nearly as may be, nor without probable cause supported by oath or affirmation.[89]

The emphasis in the Connecticut provision on "any" person or "any" place creates a broader protection for individual privacy than the same provision of the Fourth Amendment.[90] Additionally, Illinois placed an explicit protection to a right of privacy in its constitution in article I, § 6, titled "Searches, Seizures, Privacy, and Interceptions."[91] Several other states explicitly incorporate privacy into their constitutions.[92] However, the constitutional protections for computers and other

---

86 *See* FISHER, *supra* note 34, at 8.

87 *See* Jeffrey M. Shaman, *The Right of Privacy in State Constitutional Law*, 37 RUTGERS L. J. 971, 974–75 (2006).

88 CONN. CONST. art. I, § 7.

89 *Id.* (emphasis added).

90 *See id.*

91 ILL. CONST. art. I, § 6.

> The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized. *Id.*

92 Examples of states expressly protecting privacy include Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. *See* ALASKA CONST. art. I, § 22; ARIZ. CONST. art II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, §§ 12, 23; HAW. CONST. art. I, §§ 6, 7; ILL. CONST. art. I, §§ 6, 12; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

technologies that go above and beyond what the Fourth Amendment provides are rare.[93]

Furthermore, the Washington Supreme Court recently held that the private-search doctrine was inapplicable under Washington's constitution.[94] The Washington Supreme Court asserted that the protection guaranteed by the privacy provisions of the state constitution[95] are fundamentally different from the provisions found in the federal version of the Fourth Amendment.[96] Similarly, the Supreme Court of New Mexico held that the search-and-seizure provision found in New Mexico's constitution[97] has a more-stringent standard for requiring warrants than the Fourth Amendment.[98]

---

93 *See* Weaver, *supra* note 24, at 1134–35
(The steady onslaught of technology has raised troubling implications for individual privacy. While various federal and state laws might be used to maintain and protect privacy, including anti-hacking and anti-wiretapping laws, an important bulwark against the government and the police has always been the Fourth Amendment to the United States Constitution. While the Fourth Amendment has been interpreted to provide citizens with some protection against modern technologies, early United States Supreme Court decisions dealing with technology and the Fourth Amendment tended to adhere to more traditional views of the Fourth Amendment and were virtually unresponsive (except in the dissents) to the problems presented by new technologies.).

94 State v. Eisfeldt, 185 P.3d 580, 585–86 (Wash. 2008) ("We therefore reject the private-search doctrine and adopt a bright line rule holding it inapplicable under article I, section 7 of the Washington Constitution.").

95 WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

96 *See Eisfeldt*, 185 P.3d at 585–86.

97 N.M. CONST. art. II, § 10
(The people shall be secure in their persons, papers, homes and effects, from unreasonable searches and seizures, and no warrant to search any place, or seize any person or thing, shall issue without describing the place to be searched, or the persons or things to be seized, nor without a written showing of probable cause, supported by oath or affirmation.).

98 *See* State v. Rivera, 241 P.3d 1099, 1106–07 (N.M. 2010)
(We decline to retreat from our precedent which interprets Article II, Section 10 as having a stronger preference for a warrant than the Fourth Amendment. This approach honors the state's interest in encouraging private citizens to assist police officers, yet safeguards the preference for a warrant when the government seeks to search private property. This approach does not impose any greater burdens on law

These protective state measures are even more important when the sole remedy for a Fourth Amendment violation, the exclusionary rule, comes into play.[99] The exclusionary rule prohibits the use of evidence that police improperly and illegally obtained from being used at trial.[100] The main goal of the exclusionary rule is simply to deter police misconduct.[101] However, the debate over whether the rule is effective enough continues because the rule does not always apply when there is a Fourth Amendment violation,[102] leaving the person whose Fourth Amendment rights were violated without remedy.[103] Thus, this reactive measure is falling short when applied to the privacy issues involved with new technology and the private-search doctrine, specifically the uncertainty of the private-search

---

> enforcement, since for decades law enforcement officers in New Mexico have sought warrants despite their belief that they had probable cause to believe a package contained contraband.).

99 *See* Ariz. v. Evans, 514 U.S. 1, 10 (1995) (stating the Supreme Court "ha[s] recognized, however, that the Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands").

100 *See* Herring v. United States, 555 U.S. 135, 139 (2009) (stating that the Supreme Court's "decisions establish an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial").

101 *See* Kenneth W. Starr & Audrey L. Maness, *Is the Exclusionary Rule a Good Way of Enforcing Fourth Amendment Values?: Reasonable Remedies and (or?) the Exclusionary Rule*, 43 TEX. TECH L. REV. 373, 381–82 (2010).

102 *See* William Stuntz, *The Virtues and Vices of the Exclusionary Rule*, 20 HARV. J.L. & PUB. POL'Y 443, 444 (1997)

> (The exclusionary rule generates a lot of litigation—tens of thousands of contested suppression motions each year. That litigation is displacing something else, and the something else may well have more to do with guilt and innocence. That problem is much more serious than the occasional drug dealer whose Fourth Amendment claim is a ticket to get out of jail: the point is that the exclusionary rule skews the many cases in which drug dealers lose, not just the few that they win. The bottom line is not clear. The literature on this subject (on both sides) tends to assume that this is an easy issue, that suppressing illegally seized evidence is either obviously good or obviously bad. In truth, it is neither. The exclusionary rule is, by a wide margin, the best legal tool available for regulating the police. But it distorts the rest of the criminal justice system. Perhaps this argues for keeping the rule, but within fairly narrow bounds—a direction in which the law has been moving for the past two decades.).

103 *See Herring*, 555 U.S. at 140 ("The fact that a Fourth Amendment violation occurred—i.e., that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies."). S*ee also* Illinois v. Gates, 462 U.S. 213, 223 (1983).

doctrine as applied to computers, which makes it less likely for the exclusionary rule to apply.[104]

Overall, numerous scholars assert that privacy concerns are overlooked when the contents of computers are involved.[105] While Congress has passed several acts purporting to protect privacy,[106] change will be most effective on a state level until the Supreme Court renders a decision regarding the proper application of the private-search doctrine in the context of computers.[107] With the proactive changes on the state level, what is more certain than ever before is that the "abuses that led to the drafting of the Fourth Amendment have not been abated, they have merely been transformed"[108] in this new digital landscape. New abuses and privacy concerns are clearly shown with the application of the private-search doctrine to modern computers due the vast amounts of information they contain, and certain approaches, such as the virtual file-or-folder-level approach, are better suited to safeguard this privacy.[109]

II. APPLICATION OF THE PRIVATE-SEARCH DOCTRINE TO COMPUTERS

"BIG BROTHER IS WACTHING YOU."[110]

Just as in George Orwell's *Nineteen Eighty-Four*, there is a very real threat in this age of new emerging technology that Americans will slide into an Orwellian reality, where there is too much government intrusion into the privacies of life at the expense of a free society.[111] Even though tangible or physical

104 *See Herring*, 555 U.S. at 140–41.

105 *See* Shah, *supra* note 80, at 251–52.

106 *See* Fraud and Related Activity in Connection with Computers, 18 U.S.C.A. § 1030 (West 2008); Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited, 18 U.S.C.A. § 2511 (West 2008); Unlawful Access to Stored Communications, 18 U.S.C.A. § 2701 (1986).

107 *See Evans*, 514 U.S. at 10 (stating that the Supreme Court's "decisions establish an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial").

108 James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809, 2858 (2011).

109 *See* Kerr, *supra* note 5, at 556.

110 GEORGE ORWELL, NINETEEN EIGHTY-FOUR 5 (1949).

111 *See* Robert H. Thornburg, Comment, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUTER & INFO. L. 321, 321 (2002).

invasions of privacy are the main evil the Fourth Amendment attempts to ameliorate, the Amendment also attempts to protect against intangible invasions of privacy.[112] Additionally, "the more privacy an individual surrenders to private actors, the less privacy he will have from the government."[113] The advent of new technology, including faster computers and cell phones, has become such a "pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[114] Examination of the history and development of the private-search doctrine sheds light on the new privacy issues faced today.

A. Private-Search Doctrine: History and Application Challenges in an Era of Computer Crime

The private-search doctrine exception to the Fourth Amendment's warrant requirement was first articulated in *Burdeau v. McDowell*,[115] in which the Court held that the Fourth Amendment does not apply to the actions and searches of private individuals.[116] However, the seminal private-search case is *United States v. Jacobsen*,[117] where the Court outlined limitations to the expansive private-search doctrine and how far beyond the initial private search the government could go. In *Jacobsen*, employees of a freight company observed a white powdery substance that was located within a damaged container and "concealed within eight layers of wrappings."[118] The employees then contacted the Drug Enforcement Administration, and a federal agent, without a warrant, determined that the substance was cocaine in a field test of the substance.[119] Any "additional invasions of respondents' privacy by the government agent [had to] be tested by the degree to which [the government] exceeded

---

112 *See* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 122–23 (2011) (quoting United States v. United States District Court, 407 U.S. 297, 313 (1972)).

113 Sam Kamin, *Little Brothers Are Watching You: The Importance of Private Actors in the Making of Fourth Amendment Law*, 79 DENV. U. L. REV. 517, 517 (2002) (discussing "the interrelationship between privacy vis-à-vis private actors and privacy vis-à-vis the government").

114 *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014).

115 Burdeau v. McDowell, 256 U.S. 465, 475–76 (1921).

116 *See id.* at 475.

117 *Jacobsen*, 466 U.S. at 120.

118 *Id.* at 111.

119 *See id.*

the scope of the private search.[120] This is the "virtual certainty" requirement,[121] which requires that the scope of the search stay within the bounds of initial private search. The Court held that the removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search. It infringed no legitimate expectation of privacy and hence was not a "search" within the meaning of the Fourth Amendment.[122] Therefore, the search conducted by the government agent did not constitute a search under the Fourth Amendment because the inspection stayed within the initial private search and did not infringe on any expectation of privacy.[123]

Recently, in a landmark decision concerning cell phones and computers, the Supreme Court stressed how these new technologies are different from the physical containers seen in *Jacobsen* due to the amount of information they can hold.[124] In *Riley v. California*, David Riley was stopped for a traffic violation and arrested on weapons charges.[125] While searching Riley incident to the arrest, police seized a cell phone.[126] A police officer accessed the information on the cell phone, and the officer noticed the repeated use of a term associated with a local street gang.[127] The Court held that generally police may not, without a warrant,

---

120 *See id.* at 115 ("The reasonableness of an official invasion of the citizen's privacy must be appraised on the basis of the facts as they existed at the time the invasion occurred.").

121 *Id.* at 119.

122 *Id.* at 120.

123 *Jacobsen*, 466 U.S. at 143 ("Under these circumstances, therefore, respondents had no reasonable expectation of privacy in the identity of the powder, and the use of the chemical field test did not constitute a 'search' violative of the Fourth Amendment.").

124 *See Riley*, 134 S. Ct. at 2489

> (The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. 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.).

125 *See id.* at 2480.

126 *See id.*

127 *See id.*

search digital information on a cell phone belonging to an individual who has been arrested.[128] The Court noted how cell phones are like "minicomputers" and have many other functions than that of a telephone.[129] "One of the most notable distinguishing features of modern cell phones is their immense storage capacity. 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."[130] The Court stressed that the "'ultimate touchstone of the Fourth Amendment is reasonableness'" and that "'reasonableness generally requires the obtaining of a judicial warrant.'"[131] Additionally, the Court stressed it would be "unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment"[132] and that legislation and state measures are better avenues for change than federal courts in this new era of technology in protecting privacy.[133]

It is important to note that a computer is not protected against all searches.[134] Despite the challenges faced in the application of the private-search doctrine, police may usually obtain a warrant to expand upon an initial private search.[135] A majority of the cases pertaining to the private-search doctrine involve electronic

---

128 *See id.* at 2485.

129 *See id.* at 2489 (stating that "[t]hey could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers").

130 Riley, 134 S. Ct. at 2489.

131 *Id.* at 2482 (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

132 *Id.* at 2497.

133 *See id.* at 2497–98 ("Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.").

134 *Id.* at 2493 ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").

135 *See* Coolidge v. N. H., 403 U.S. 443, 481 (1971)

> (The warrant requirement has been a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be somehow 'weighed' against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' who are a part of any system of law enforcement.).

child-pornography cases.[136] Disturbing and unpredictable results are evident with the use of the private-search doctrine in this era of computer crime, including the increasing use of viruses that can enter an individual's computer when he simply visits a website, opens an email or attachment, or shares music, files, and photos with others.[137] Child pornography, or evidence of another crime, could end up unknowingly on an individual's computer due to a person's attempt to frame someone and plant electronic evidence.[138]

For instance, in just one example, an Internet virus made one Massachusetts's man named Michael Fiola a collector of child pornography because "[h]einous pictures and videos can be deposited on computers by viruses."[139] Fiola fought the charge by spending $250,000 on legal fees, and suffered unquantifiable damage to his reputation.[140] Further investigation later revealed

> the laptop was severely infected. It was programmed to visit as many as 40 child porn sites per minute – an inhuman feat. While Fiola and his wife were out to dinner one night, someone logged on to the computer, and porn flowed in for an hour and a half.[141]

After almost a year, Fiola's charges were dropped, but "[c]omputers are not to be trusted"[142] because with new technology the potential for abuse by law enforcement as well as private third parties increases.[143] There are several cases where

---

136 *See* Shah, *supra* note 80, at 255.

137 *See Computer Virus Information*, WEBROOT, http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses (last visited Feb. 18, 2016).

138 *See* Mike Rigby, *Child Porn Investigations May Snare the Innocent*, PRISON LEGAL NEWS (Nov. 15, 2010), https://www.prisonlegalnews.org/news/2010/nov/15/child-porn-investigations-may-snare-the-innocent/.

139 *See* Jordon Robertson, *Viruses Can Turn PCs into Child-porn Servers*, THE BOSTON GLOBE (Nov. 9, 2009), http://archive.boston.com/business/technology/articles/2009/11/09/viruses_can_turn_pcs_into_child_porn_servers/.

140 *See id.*

141 *Id.*

142 *Id.*

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

> (As with any Fourth Amendment inquiry, we must weigh the government's interest in conducting the search of Lichtenberger's property against his privacy interest in that property. That the item in question is an electronic device

the defendants have not been responsible for the information found on their computers,[144] and their privacy has been violated by government intrusion.[145]

A chief rationale for the private-search doctrine exception is that by conducting a search subsequent to a private search, law enforcement is not learning anything new that they did not already know as a result of what was disclosed by the initial search.[146] However, the information searched and viewed may no longer be private, but that does not mean all information should be discoverable.[147] The government's ability to easily intrude on an individual's privacy stresses the need for a more narrow and cautious approach in utilizing the private-search doctrine.[148] An individual's personal property can be easily hacked with current technology, which can make digital evidence discovered on a computer questionable in what it brings to light.[149] The Sixth Circuit's recent application of the virtual file-or-folder-level approach in *United States v. Lichtenberger*[150] may not be a narrow enough application of the doctrine, but it is currently the best solution in order to protect an individual's privacy from unreasonable searches and seizures in an age of new technologies and security threats.[151]

B. Virtual File-or-Folder-Level Approach

In the most recent and vital case concerning the private-search doctrine, and its application to computers, the Sixth Circuit favored a virtual file-or-folder-level approach in order to best

---

> does not change the fundamentals of this inquiry. But under *Riley*, 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.).

144 *See* Robertson, *supra* note 139 (stating that "[i]n one case, an infected e-mail or pop-up ad poisoned a defense contractor's PC and downloaded the offensive pictures").

145 *See id.*

146 *See Jacobsen*, 466 U.S. at 115 ("The additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search.").

147 *See* Holley, *supra* note 22, at 715 ("The private search exception is premised on the idea that items searched by a third party are no longer private.").

148 *See infra* Section III.A.

149 *See* Robertson, *supra* note 139.

150 *See Lichtenberger*, 786 F.3d at 485, 490–91.

151 *See infra* Section III.A.

safeguard individual privacy from unwanted and unwarranted government intrusion.[152] In *United States v. Lichtenberger*, Aron Lichtenberger was initially arrested for failing to register as a sex offender;[153] however, following his arrest, Lichtenberger's girlfriend hacked into his computer, changed his password, and found images of child pornography.[154] Acting as a private party, Lichtenberger's girlfriend notified law enforcement of her discovery and showed police the digital evidence of child pornography on Lichtenberger's personal laptop computer.[155]

However, the Sixth Circuit suppressed this evidence as the product of an unconstitutional search[156] because when police arrived and asked Lichtenberger's girlfriend to reproduce her previous search, she could not remember which files and folders she had looked through.[157] The danger of this result, which the court was trying to prevent, was that law enforcement could have discovered something unrelated to the initial search on Lichtenberger's personal computer that was private, and completely unrelated to child pornography.[158] There was no "virtual certainty" that the images shown to police would contain images of child pornography as opposed to something else personal, such as bank statements or other private communications.[159] Therefore, the court focused on the scope of

---

152 *See Lichtenberger*, 786 F.3d at 485.

153 *Id.* at 479.

154 *Id.*

155 *Id.* at 479–80.

156 *See id.* at 491

> (In light of the information available at the time the search was conducted, the strong privacy interests at stake, and the absence of a threat to government interests, we conclude that Officer Huston's warrantless review of Lichtenberger's laptop exceeded the scope of the private search Holmes had conducted earlier that day, and therefore violated Lichtenberger's Fourth Amendment rights to be free from an unreasonable search and seizure. The laptop evidence and evidence obtained pursuant to the warrant issued on the basis of its contents must be suppressed.).

157 *See id.* at 481 ("Holmes also testified that she showed Officer Huston 'a few pictures' from these files, although she was not sure if they were among the same images she had seen in her original search.").

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

159 *Id.*

> (The same folders—labeled with numbers, not words—could have contained, for example, explicit photos of Lichtenberger himself: legal, unrelated to the crime alleged, and the most private sort of images. Other documents, such as bank

the police officer's search vis-à-vis the initial private search, and whether there was a "near-certainty regarding what [police] would find and little chance to see much other than contraband."[160] Finally, the court did not adopt the whole-computer approach because current technology, including computers, greatly increases the privacy interests at stake, which tips the balance in favor of the individual's privacy interest over the governmental interest.[161]

Moreover, a recent decision from the Eleventh Circuit has deepened the circuit split between the whole-computer approach, and the virtual file-or-folder-level approach, making the issue even riper for review because a petition for certiorari has been filed.[162] In *United States v. Johnson*,[163] the Eleventh Circuit appeared to adopt the virtual file-or-folder-level approach on how to apply the private-search doctrine of the Fourth Amendment to computers as seen in *Lichtenberger*.[164] In *Johnson*, defendants Robert Alan Johnson and Jennifer Sparks left a cell phone at a Walmart that contained hundreds of images and videos of child pornography.[165] A Walmart employee looked at the phone, which

---

> statements or personal communications, could also have been discovered among the photographs. So, too, could internet search histories containing anything from Lichtenberger's medical history to his choice of restaurant. The reality of modern data storage is that the possibilities are expansive.)

160 *Id.* at 486
> (We have held a government search permissible—that is, properly limited in scope—in instances involving physical containers and spaces on the grounds that the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband.).

161 *See id.* at 488
> (As with any Fourth Amendment inquiry, we must weigh the government's interest in conducting the search of Lichtenberger's property against his privacy interest in that property. That the item in question is an electronic device does not change the fundamentals of this inquiry.).

162 Orin Kerr, *11th Circuit Deepens the Circuit Split on Applying the Private Search Doctrine to Computers*, WASH. POST: THE VOLOKH CONSPIRACY, Dec. 02, 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/.

163 United States v. Johnson, 806 F.3d 1323 (11th Cir. 2015).

164 *See id.* at 1336.

165 *See id.* at 1329.

was not password protected, and discovered the images.[166] The employee then showed her husband, who viewed the images and a video, and they alerted law enforcement.[167] Later, a police officer viewed the images, opening them up to full size, and he watched a video previously seen in the private search, as well as another video not originally viewed.[168] The court held that the police officer exceeded the scope of the initial private search when he viewed the video not originally seen, and violated the Fourth Amendment.[169]

Likewise, in the Tenth Circuit case *United States v. Carey*,[170] the relevant scope of the search concerning digital files and data was the individual file, rather than the whole computer.[171] In *Carey*, a forensic analyst was looking for evidence of drug sales, but came across pictures of child pornography on the suspect's computer.[172] However, a search warrant clearly delineated the files that could be searched had to pertain to the sale or distribution of controlled substances.[173] When the officer began to open certain files with sexually suggestive titles, he exceeded the bounds of his search of the defendant's computer for drug-related evidence.[174] Thus, the court found that the evidence seized was the product of an unconstitutional general search.[175] Additionally, the Tenth Circuit suggested an approach to deal with "intermingled documents"[176] and that law enforcement had

---

166 *See id.*

167 *See id.* at 1330–31.

168 *See id.* at 1336.

169 *See Johnson*, 806 F.3d at 1336
(But with respect to the second video, which Widner never watched, O'Reilly's review exceeded—not replicated—the breadth of the private search. Nothing in *Simpson* provides a safe harbor for a governmental search of materials beyond the scope of a private search.).

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

171 *See id.* at 1274.

172 *See id.* at 1270–71.

173 *See id.* at 1272.

174 *See id.* at 1274
(Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware—in advance of opening the remaining files—what the label meant. When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant. . . .).

175 *See id.* at 1276.

176 *Carey*, F.3d at 1275

several options in dealing with computers and digital evidence because police can avoid searching files that are not part of the previous search or identified in a warrant.[177]

Several other circuits follow the virtual file-or-folder-level approach as seen in *Lichtenberger*, *Johnson*, and *Carey*, and in each case, the court asserted that the scope of the computer search is determined by the files the private party views in an initial search or the files as specified in a warrant.[178] This narrower application of the private-search doctrine will avoid an overly exhaustive and intrusive government search into an individual's private affairs.[179] However, the other side to this debate involves the whole-computer approach as seen in decisions from the Fifth and Seventh Circuits.[180]

C. Whole-Computer Approach

> (Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.).

177 *See id.* at 1276 (stating that law enforcement can avoid search and seizure issues by "observing file[] types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory.").

178 *See, e.g.*, United States v. Tosti, 733 F.3d 816, 822 (9th Cir. 2013) (upholding evidence in a warrantless search case involving child pornography discovered by computer-repair employee because the detectives "viewed only those photos [the technician] had already viewed"); United States v. Grimes, 244 F.3d 375, 378, 383 (5th Cir. 2001) (upholding a warrantless search because "only the previously-found images" were shown to authorities); United States v. Ahrndt, Crim. No. 3:08–CR–00468–KI, 2013 WL 179326, at *23 (D. Or. Jan. 17, 2013) (suppressing evidence because deputy opened an image the private searcher had not).

179 *See* United States v. Jacobsen, 466 U.S. 109, 115 (1984) ("The additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search.").

180 *See Rann*, 689 F.3d at 838 (holding that "per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches. Because S.R. and her mother knew the contents of the digital media devices when they delivered them to the police, the police were 'substantially certain' the devices contained child pornography"); United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001) (holding that "the police in the instant case did not exceed the scope of the private search if they examined more files on the privately-searched disks than Judith and Brandie had").

The Fifth Circuit's decision in *United States v. Runyan* asserted that the whole-computer or physical-container approach is the best method for law enforcement to follow in searching an individual's computer.[181] In *Runyan*, Runyan's ex-wife searched through his physical property in order to retrieve items she believed were her own following their divorce.[182] During one of her searches, Runyan's wife discovered a bag and several boxes filled with images of child pornography stored on compact disks and computer disks.[183] On another trip, Runyan's wife took his desktop computer and surrounding disks to her residence and viewed the contents before contacting law enforcement.[184] Runyan's wife then turned over "twenty-two CDs, ten ZIP disks, and eleven floppy disks"[185] to the officer, and the police conducted a more thorough analysis of the digital evidence without a warrant that yielded more images of child pornography than Runyan's wife had seen.[186] Runyan claimed that law enforcement exceeded the previous initial search, so the private-search doctrine did not apply.[187] The court held that law enforcement did exceed the scope of the initial private search when they examined disks Runyan's wife had not viewed,[188] but they did not exceed the scope of the prior search when they viewed more on the privately searched disks than the private party.[189] The Fifth Circuit held that any additional analysis of the disks merely expanded the prior search, and even though the police had opened different files, it did not matter because the zone of the search was defined by the physical container or whole computer.[190]

The Seventh Circuit applied a similarly expansive rationale for

---

181 *See Runyan*, 275 F.3d at 464.

182 *See id.* at 452–53.

183 *See id.* at 453.

184 *See id.*

185 *Id.*

186 *See id.* at 464.

187 *Runyan*, 275 F.3d. at 460 ("Runyan argues that the private-search doctrine is inapplicable in the instant case because the police exceeded the scope of the private search. He maintains that the police's pre-warrant search of the disks exceeded the scope of the review conducted by Judith and Brandie in a number of ways.").

188 *See id.* at 464.

189 *See id.* at 465.

190 *See id.* at 464 ("In the context of a closed container search, this means that the police do not exceed the private search when they examine more items within a closed container than did the private searchers.").

the whole-computer approach in *Rann v. Atchison*.[191] In *Rann*, the defendant's daughter reported that she was a victim of child pornography.[192] The daughter later went home and obtained a memory card that contained evidence of the pornographic pictures.[193] Additionally, the defendant's wife submitted a computer zip drive that contained more digital evidence of child pornography.[194] Even though both items were viewed by law enforcement without a warrant, the court adopted the Fifth Circuit's approach in *Runyan* to find the subsequent police searches permissible.[195] Both the mother and daughter knew the content of the digital evidence they gave to the police; therefore, the police could be "substantially certain" that the items contained evidence of child pornography.[196]

The private-search doctrine has differing applications across the United States, and the zone of the search can be placed into the two different approaches, including the virtual file-or-folder-level approach or the whole-computer approach.[197] Advocates of the whole-computer approach fear a narrow application of the private-search doctrine will over-deter police from conducting a lawful search and investigation.[198] The virtual file-or-folder-level approach is preferable because computers are searched for the specific information they contain, and courts need to focus on that specific information rather than allowing for a broad search of the

---

191 *Id.* at 833–34, 838.
192 *See id.* at 834.
193 *See Runyan*, 275 F.3d. at 834.
194 *See id.*
195 *See id.* at 838.
196 *Id.*
197 *See* Kerr, *supra* note 5, at 554–55.
198 *See Runyan*, 275 F.3d at 465.

> Police would thus be disinclined to examine even containers that had already been opened and examined by private parties for fear of coming across important evidence that the private searchers did not happen to see and that would then be subject to suppression. The *Rouse* approach would over-deter the police, preventing them from engaging in lawful investigation of containers where any reasonable expectation of privacy has already been eroded. This approach might also lead police to waste valuable time and resources obtaining warrants based on intentionally false or mistaken testimony of private searchers, for fear that, in confirming the private testimony before obtaining a warrant, they would inadvertently violate the Fourth Amendment if they happened upon additional contraband that the private searchers did not see. *Id.*

entire storage device.[199] A broad search will lead to "unpredictable, unstable, and even disturbing results."[200] Thus, the virtual file-or-folder-level approach for retrieving digital evidence stored on computers provides a narrow application of the private-search doctrine in order to better safeguard individual privacy.[201]

III. PROPER ANALYSIS FOR PROTECTING INDIVIDUAL PRIVACY UNDER THE PRIVATE-SEARCH DOCTRINE

The Sixth Circuit's decision in *United States v. Lichtenberger* has created a clear circuit split with regard to private searches and computers.[202] The virtual file-or-folder-level approach advocated in that case is currently the most reasonable solution available for balancing individual privacy with computers, and the vast amounts of information they contain along with the power of law enforcement.[203] Conversely, the whole-computer approach allows a search that is too broad and leaves the entire computer open to exhaustive search by the government after a private party has viewed only a single file.[204] The whole-computer approach is not an attempt to be more thorough; it is akin to a fishing expedition.[205] The vast difference in scope between searching one file or folder versus a whole computer full of data and limitless private information is extremely dangerous.[206] Until the Supreme Court renders a clear decision regarding the proper application of the private-search doctrine, states can act individually by adopting and amending more detailed police procedures and manuals, more protective common-law decisions, and more privacy-focused constitutional provisions in order to aid in narrowing the application of the private-search doctrine to protect American citizens from overzealous

---

199 *See* Kerr, *supra* note 5, at 556.

200 *Id.* (stating that "[s]ome computer storage devices may not be stored in any boxes at all. Over time, it should become increasingly clear that the Fourth Amendment should track the information, not the physical box").

201 *See id.*

202 *See* Kerr, *supra* note 12.

203 *See* Kerr, *supra* note 5, at 556.

204 *See id.*

205 *See* Holley, *supra* note 22, at 703 ("The difference in scope undermines the spirit and intent of the private search exception. Such an act is not merely examining the computer 'more thoroughly,' but is instead fishing in entirely uncharted waters.").

206 *See id.*

government intrusion.[207]

A. The Private-Search Doctrine Must Be Applied Narrowly to Current Technology

The main rationale for the private-search doctrine exception is that by conducting a search subsequent to a private search, law enforcement is not learning anything new that they did not already know as a result of what was disclosed by the initial search.[208] Exceptions to the Fourth Amendment were created because there are specific situations where it is not practicable to obtain a warrant in time; however, these reasons cannot outweigh the Constitution's protection of the individual against the overwhelming power of the government.[209] People have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[210] With changes in lifestyle and the introduction of technology, computers are now included in this protection.[211] With these changes, there has been great debate over how best to balance an individual's right to privacy and constitutional protection under the Fourth Amendment against possibly hindering law enforcement's ability to find and arrest criminals.[212]

1. Preserving Individual Privacy

The private-search doctrine must be narrowly applied to new technologies because their expanding capacities to hold vast amounts of personal identifying information increases the privacy

---

207 *See supra* Section I.B.

208 *See* United States v. Jacobsen, 466 U.S. 109, 115 (1984) ("The additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search.").

209 *See supra* Part I.

210 *See* U.S. CONST. amend. IV.

211 *See Katz*, 389 U.S. at 353

> (The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.).

212 *See infra* Subsection III.A.2.

interests at stake.[213] This new technology contains very specific information, such as location data, political affiliation, banking history, and other privacies of life.[214] There should be a narrow application of this Fourth Amendment warrant exception because even though most of the cases involving the private-search doctrine involve child pornography,[215] the rights of the criminal that people are so willing to intrude upon today will be the rights of the average American citizen tomorrow.[216] The Framers of the Constitution could not have imagined the new search-and-seizure issues Americans face today due to new transformative technologies, but the principles behind the Fourth Amendment remain the same,[217] including an American citizen's right to be free from overzealous government intrusion into the privacy of his home and personal life.[218]

The principles behind the Fourth Amendment demonstrate Americans' foundational belief in limited government and separation of powers.[219] The historical foundations of the

---

213 *See Computers & the Internet*, *supra* note 2 and accompanying text.

214 *See Riley*, 134 S. Ct. at 2489.

> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. *Id.*

215 *See* Shah, *supra* note 80, at 255–56.

216 *See* Palumbo, *supra* note 8, at 979–80.

217 *See* Kerr, *supra* note 5, at 538 ("Computer searches and home searches are similar in many ways. In both cases, the police attempt to find and retrieve useful information hidden inside a closed container.").

218 *See id.* at 536.

> General warrants permitted the King's officials to enter private homes and conduct dragnet searches for evidence of any crime. The Framers of the Fourth Amendment wanted to make sure that the nascent federal government lacked that power. To that end, they prohibited general warrants: every search or seizure had to be reasonable, and a warrant could issue under the Fourth Amendment only if it particularly described the place to be searched and the person or thing to be seized.

219 *See* Shih Ray Ku, *supra* note 38, at 1326.

Amendment make clear that while privacy was a concern in drafting the Amendment, the main fear was "unfettered governmental power and discretion."[220] Searches occurring today involving new technologies are still the very searches the Framers of the Fourth Amendment feared, as there is still a very serious threat working to erode privacy.[221] Just because there are no physical intrusions of something material and tangible as seen in *Olmstead v. United States*[222] with technology today, Fourth Amendment principles should continue to act as a shield to the increasing number of unreasonable searches and seizures of technology conducted by private parties and law enforcement. *Katz v. United States* rejected *Olmstead's* narrow focus on tangible and physical intrusions[223] and took a step in the right direction by considering technology in search-and-seizure cases while protecting individual privacy.[224] Additionally, in order to

---

> [T]he amendment is best understood as a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens. The amendment does so as part of the rich tapestry that is the Constitution, and cannot be viewed in isolation, but must at the very least be viewed together with the principles embodied in the constitutional separation of powers.

220 *Id.* at 1332 ("[W]hile privacy in terms of the sanctity of home and papers was a concern prior to the amendment's adoption, the overarching concern was unfettered governmental power and discretion, and that 'the people' played a prominent role in defining the scope of government power and limiting its exercise.").

221 *See id.* at 1343.

222 *See Olmstead*, 277 U.S. at 466.

> Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure. We think, therefore, that the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment. *Id.*

223 *See Katz*, 389 U.S. 353 ("We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

224 *See id.* at 361 (explaining the twofold requirement for a search: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

continue to support these principles of limited government, separation of powers, and individual privacy, warrant exceptions such as the private-search doctrine must be drafted as narrowly as possible.[225] Otherwise, there will be a dangerous expansion of the government's investigative power.[226] Privacy and security decisions must be left to "the people"[227] in order to avoid a severe power shift to the government. Thus, the whole-computer approach would undermine the principles of the Fourth Amendment by expanding government power and discretion rather than limiting its scope.[228]

Additionally, the narrow interpretation of the private-search doctrine does not hinder the government's ability to find and arrest criminals just because the doctrine fails to give a green light to law enforcement to repress individual privacy in the name of collecting evidence. All law enforcement has to have is probable cause—a very low bar—to obtain a warrant for anything beyond the initial private search.[229] Thus, law enforcement powers are not hindered because if probable cause exists, then police can easily obtain a search warrant from a judge for any further searches.[230] Also, by making sure law enforcement is properly trained in the investigation and collection of digital evidence through more specific guidelines, evidence of a crime will not need to be excluded or suppressed later.[231]

Another example of where a broad application of the private-search doctrine is troubling is if an overzealous prosecutor goes after a business or individual on one charge, but conducts a wider search for all evidence of criminal wrongdoing.[232] A narrow

---

225 *See supra* Section III.A.

226 *See* Shih Ray Ku, *supra* note 38, at 1326 ("[T]he Supreme Court has shifted the authority for determining the scope of government's investigative power from the people to judges and law enforcement.").

227 U.S. CONST. pmbl.

228 Shih Ray Ku, *supra* note 38, at 1357 ("The Founders also believed that the people should play a significant role in making this determination. The Supreme Court's current approach does more than ignore these concerns–it undermines them.").

229 *See* Holley, *supra* note 22, at 716.

230 *See id.*

231 *See supra* Section I.B.

232 *See* Palumbo, *supra* note 8, at 993.

> Indeed, one can easily imagine an overzealous U.S. Attorney seeking a warrant for 'financial records' on a large bank's computer system and then engaging in a wholesale search for any and all evidence of criminal activity. Perhaps the only saving grace to privacy rights hidden in this rationale is that

application of the private-search doctrine does not handicap law enforcement; it keeps police accountable for obtaining warrants for information beyond the scope of the initial private search and protects an individual's reasonable expectation of privacy to be free from government intrusion.[233] It is important to be aware that rights infringed on today for a suspected criminal could be restricted for the average law-abiding citizen in the future.[234]

Therefore, a narrow application of the private-search doctrine through the virtual file-or-folder-level approach will only result in keeping a check on overzealous government intrusion and law enforcement action.[235] These protections will not hinder law enforcement's ability to do their job because it is simply reestablishing the principles that American society should already be abiding by, including the right to be free from unreasonable searches and seizures and to enjoy the implicit right to some privacy.[236] The private-search doctrine is an exception to the warrant requirement, and law enforcement has many other tools and exceptions at its disposal to offset any minor burdens in conducting their duties.[237] Other opposition is likely to come from proponents of the whole-computer approach for the private-search doctrine.[238]

2. The Private-Search Doctrine Would Become Too Broad to Be Constitutional

There needs to be a narrow application of the private-search doctrine because it would be too broad otherwise to be constitutional. By taking a narrower virtual file-or-folder-level approach to searching computers rather than searching the whole computer, law enforcement can avoid unstable, intrusive, and illegal results in subsequent searches.[239] Everything on a

incriminating evidence may possibly be suppressed if a judge finds ex post that it was discovered improperly. Whether or not this protection is enough to adequately safeguard privacy rights, however, is debatable.

233 *See* Holley, *supra* note 22, at 717.

234 *See* Palumbo, *supra* note 8, at 979–80.

235 *See supra* Section I.B; *supra* Section II.B.

236 *See* Shih Ray Ku, *supra* note 38 and accompanying text.

237 *See* Holley, *supra* note 22, at 717.

238 *See supra* Section II.C.

239 *See* Kerr, *supra* note 5, at 556 ("Some computer storage devices may not be stored in any boxes at all. Over time, it should become increasingly clear that the Fourth Amendment should track the information, not the physical

computer is not always relevant for the purposes of a law enforcement investigation.[240] For instance, in *Lichtenberger*, when Lichtenberger's girlfriend tried to reproduce her previous private search for law enforcement, she could not remember which files and folders she had initially looked through.[241] The danger with these results, as the court determined, was that the police could have discovered something unrelated to that initial search on Lichtenberger's computer that was private, and completely unrelated to child pornography.[242] Thus, law enforcement should carefully ask the private party to show files that the private party previously viewed in order to replicate the search rather than expand on the initial search.

Additionally, supporters of a broad whole-computer approach are focused on preventing the destruction of evidence.[243] However, as discussed in *Riley v. California*, there are more targeted ways to prevent the loss of evidence in a critical and time-sensitive situations by relying on exigent circumstances to search everything immediately.[244] Most private-search doctrine cases are not unpredictable arrest situations because when the private party discovers the incriminating evidence, the individual is likely not aware that his privacy has been violated.[245] Also, law enforcement can obtain a warrant after performing a cursory search based on the private search, and the police can use more specific language in that later warrant to clarify what law enforcement intends to seize and what they plan to search for in the electronic search of the computer.[246] In *United States v. Carey*, the Tenth Circuit asserted that law enforcement has

---

box.").

240 *See id.*

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

242 *See id.* at 488–89.

243 *See Riley*, 134 S. Ct. at 2486.

244 *See id.* at 2487 ("To the extent that law enforcement still has specific concerns about the potential loss of evidence in a particular case, there remain more targeted ways to address those concerns.").

245 *See id.* at 2488.

246 *See* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 132 (2005).

> In digital evidence cases, more specific language should be used. The language should require the police to state what physical evidence they plan to seize on-site, and then indicate what kind of evidence they plan to search for in the subsequent electronic search. In other words, agents should be required to describe the property to be seized at *both* the physical search stage *and* the electronic search stage. *Id.*

several options in dealing with digital evidence and computers because they can avoid searching folders and files that are "not identified in the warrant: observing file[] types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[247] Therefore, a narrower search for the relevant digital evidence is quite feasible.

Some courts have found that the whole-computer approach as opposed to the virtual file-or-folder-level approach is more desirable because the whole-computer approach is a much more simple application of basic search-and-seizure law.[248] However, by allowing government to search the whole computer, too much personal information is at stake, and this approach will result in unwarranted intrusions into an individual's life.[249] This information could be bank statements, addresses, photographs, or browsing history.[250] The landmark Supreme Court decision in *Riley v. California* began the process of expanding Fourth Amendment protection to digital information stored in cell phones and computers.[251] Also, the Eleventh Circuit applied this

---

247 *Carey*, 172 F.3d at 1276.

248 *See* Goldfoot, *supra* note 112, at 158 ("The physical perspective also permits the straightforward application of existing search and seizure law.").

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

250 *See id.* S*ee also* Kerr, *supra* note 5, at 543.

> Common word processing programs such as WordPerfect and Microsoft Word generate temporary files that permit analysts to reconstruct the development of a file. Word processing documents can also store data about who created the file, as well as the history of the file. Similarly, browsers used to surf the World Wide Web can store a great deal of detailed information about the user's interests, habits, identity, and online whereabouts, often unbeknownst to the user. Browsers typically are programmed to automatically retain information about the websites users have visited in recent weeks; users may use this history to retrace their steps or find webpages they previously visited. Some of this information may be very specific; for example, the address produced by an Internet search engine query generally includes the actual search terms the user entered. *Id.*

251 *See Riley*, 134 S. Ct. at 2490

> (Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease,

reasoning to cell phones in *United States v. Johnson*[252] when the court held that the police officer exceeded the scope of the initial private search and violated the Fourth Amendment when he viewed a video not originally seen on the defendants' cell phone.[253] With the introduction of technology, search-and-seizure law can no longer remain stagnant. The ideas that the Framers embedded in the Fourth Amendment must transform with these new technologies in order to preserve the basic concept behind the Amendment and to safeguard a reasonable expectation of privacy.[254] Some states have laws, policies, and constitutions that reflect this sentiment.[255]

Proponents of the whole-computer approach may also argue that an individual's expectation of privacy has already been compromised by the private searchers, so the police are not exceeding the initial private search by examining the computer more thoroughly than the initial searcher.[256] This idea has been

---

> coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.).

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

253 *See id.* ("But with respect to the second video, which Widner never watched, O'Reilly's review exceeded—not replicated—the breadth of the private search. Nothing in Simpson provides a safe harbor for a governmental search of materials beyond the scope of a private search.").

254 *See* Shih Ray Ku, *supra* note 38, at 1362

> (As it stands, under the Court's current approach [to the Fourth Amendment and technology], the people play absolutely no role in determining the extent and reasonableness of government's power to search. Instead, the Court treats law enforcement as having unfettered government power to invade individual privacy and security subject only to a few not so well defined but limited exceptions defined by the Court. Whatever role the Fourth Amendment might have played in regulating executive power consistently with the doctrine of separation of powers, in many instances it currently plays no role whatsoever. This state of affairs is precisely what the Founders feared most.).

255 *See supra* Section I.B.

256 *See Runyan*, 275 F.3d at 464–65

> (We agree with the Eleventh Circuit's position in *Simpson* that the 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. In the context of a

espoused in the Fifth and Seventh Circuits but is at odds with safeguarding individual privacy.[257] A narrow application of the private-search doctrine is vital because with current technology there can be serious doubts and questions raised concerning how the evidence of criminal wrongdoing actually found its way on an individual's computer.[258] With new technology, the potential for abuse by not only law enforcement, but also by private parties dangerously increases the privacy interests at stake.[259] With the increased use of viruses and other computer crimes, there are numerous instances where an individual can pick up photos of child pornography or evidence of another crime simply by visiting a website or opening an email.[260] A private party could take advantage of the private-search doctrine by planting evidence of a crime on the computer of another person and then showing police.[261] Thus, there is a danger that evidence found on a computer may not even be known to the owner of that computer,[262] so law enforcement should use a more cautious approach when gleaning information from a private search.

Another possible objection to a narrow interpretation of the private-search doctrine is that somehow there could be an incentive for a private searcher to examine more files and folders in the initial search in order to avoid the issue of not showing law enforcement enough evidence.[263] However, most people do not

---

> closed container search, this means that the police do not exceed the private search when they examine more items within a closed container than did the private searchers.).

257 *See id. See also Rann*, 689 F.3d at 838.

258 *See* Mantei, *supra* note 7, at 987 ("Computers are also changing the methods of criminal conduct. Users can easily store evidence of both petty offenses and complex enterprises in file folders with family pictures, research papers, digital music, and other benign materials.").

259 *See Lichtenberger*, 786 F.3d at 488

> (As with any Fourth Amendment inquiry, we must weigh the government's interest in conducting the search of Lichtenberger's property against his privacy interest in that property. That the item in question is an electronic device does not change the fundamentals of this inquiry. But under *Riley*, 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.).

260 *See* Rigby, *supra* note 138 (explaining how an Internet virus made one Massachusetts's man named Michael Fiola a collector of child pornography).

261 *See id.*

262 *See id.*

263 *See* Holley, *supra* note 22, at 716.

have knowledge of these evidentiary rules, and they are most likely going to stumble upon any evidence of criminal conduct unless they are involved in planting the evidence on the individual's computer.[264] In the end, it is preferable for the private party to recreate her search than to allow government to peruse random files and conduct their own exhaustive search.[265]

The narrow application of the private-search doctrine is necessary to preserve individual privacy because there are serious privacy interests at stake due to the increased storage capacity of current technology.[266] Also, a narrow application of the doctrine is needed because otherwise the private-search doctrine will be too broad to be constitutional, especially when there are serious questions concerning the nature and source of evidence on an individual's computer.[267] Finally, with the similarities between home searches and computer searches, the narrow application of the doctrine will help avoid the dangers of an overbroad granting of power to the government, which will avoid intrusive and disturbing results.[268] The narrow application of the private-search doctrine is best achieved through the virtual file-or-folder-level approach, but until the Supreme Court renders a decision regarding the proper approach and resolves the circuit split, states can take other protective measures to control abuse of individual privacy.[269]

B. Solutions Regarding Application of the Private-Search Doctrine to Computers

The Supreme Court has not yet provided clear authority on how the private-search doctrine should apply to new technologies, so the struggle will continue at the state level until the Court acts.[270] In the meantime, states should narrowly apply the private-search doctrine by adopting more protective measures.[271]

---

264 *See id.*

265 *See id.*

266 *See Lichtenberger*, 786 F.3d at 488–89. *See also* Kerr, *supra* note 5, at 542 ("Computer operating systems and programs also generate and store a wealth of information about how the computer and its contents have been used. As more programs are used, that information, called metadata, becomes broader and more comprehensive.").

267 *See* Rigby, *supra* note 138.

268 *See* Kerr, *supra* note 5, at 556.

269 *See supra* Section I.B, at 12.

270 *See supra* Section I.B, at 15.

271 *See supra* Section I.B, at 13.

There already is a trend among numerous states to create more protections against unreasonable searches and seizures as they apply to computers and digital evidence through computer-specific rules and procedures in police manuals, common-law decisions, and implementation of more protective articles concerning searches and seizures in state constitutions.[272] These steps can aid in the narrow application of the private-search doctrine.[273]

First, experts at the state level should work with local and county law enforcement to adapt to these emerging technologies while continuing to respect individual privacy, but still target individuals using these technologies for criminal purposes.[274] It is vital, with the increase in computer crime, that law enforcement understands how best to seize electronic evidence from computers and other modern technologies.[275] Each state can accomplish this objective by coordinating to create a computer-evidence search-and-seizure manual to provide guidance to all involved in this new technology setting.[276] Such manuals are used by New Jersey and Ohio to help define the current search-and-seizure issues, including the proper application of the private-search doctrine, and the limits to such a search.[277] For instance, the New Jersey manual provides detailed guidance and steps that police should take in seizing any computer evidence in situations where a warrant-based search and seizure is involved or where warrantless searches and seizures occur.[278]

---

272 *See supra* Section I.B, at 12.

273 *See supra* Section I.B, at 15.

274 *See* DEP'T OF LAW & PUB. SAFETY DIV. OF CRIMINAL JUSTICE, *supra* note 81, at 2.

275 *See* OFF. OF LEGAL EDUC., *supra* note 83, at ix.

276 *See* DEP'T OF LAW & PUB. SAFETY DIV. OF CRIMINAL JUSTICE, *supra* note 81, at 1. *See also* OFF. OF LEGAL EDUC., *supra* note 83, at vii.

277 *See supra* Section I.B, at 12.

278 *See* DEP'T OF LAW & PUB. SAFETY DIV. OF CRIMINAL JUSTICE, *supra* note 81, at 47–49

> (In determining what action should be taken in regard to computer evidence discovered at the scene but not within the scope of the warrant, it may be appropriate to consider how much data may be stored on the computer, which conceivably could store all of a business's records. If a huge amount of data outside of the scope of the warrant is seized and a court finds that the warrantless seizure was invalid, it potentially could conclude that seizure of the computer and its contents constituted a 'general search' and suppress all of the evidence seized.).

Also, the federal Office of Legal Education Manual provides suggestions and discussion concerning the current status of the law for seizing electronic evidence.[279] Specifically, the manual focuses on private searches and an individual's reasonable expectation of privacy.[280] This manual is a clear example of what type of manual should be adopted at the state level.[281] State manuals should have specific sections dedicated to the Fourth Amendment's reasonable expectation of privacy in cases involving computers and discussion concerning private searches.[282] These manuals can inform and train law enforcement and prosecutors in the current law surrounding private searches and the specific procedures for collecting computer-related evidence.[283] While all states have statutes regarding computer crime, more specific rules and guidelines can be provided to law enforcement and prosecutors through the collaboration of experts at the state level in training all involved in how to handle computer searches, and the legal issues that arise.[284] Due to the relative ease with which evidence can be seized, and the intimate individual information involved, a statutory response may also need to be instituted by the state to create a more protective search-and-seizure law specifically for computers.

Next, states can make binding rules for law enforcement through common-law decisions, and each state can interpret the search-and-seizure requirements of their constitutions to prohibit disturbance of a person's private affairs without the authority of law by focusing on rights of the individual rather than on the reasonableness of the government action.[285] For instance, in *State v. Eisfeldt*,[286] the Washington Supreme Court found the private-search doctrine was inapplicable under the state's constitution and that the state constitution's privacy provisions were more protective than those provided by the Fourth Amendment.[287] Specifically, Article I, § 7 of the Washington Constitution begins with a broader inquiry into whether the

279 *See* OFF. OF LEGAL EDUC., *supra* note 83, at ix–xii.
280 *See id.* at 2–10.
281 *See id.* at ix–xii
282 *See id.* at 1–13.
283 *See id.* at ix–xii.
284 *See supra* Section I.B, at 11–12.
285 *See supra* Section I.B.
286 *Eisfeldt*, 185 P.3d at 586.
287 *See id.* at 586.

government has intruded into a person's "private affairs."[288] "Unlike the Fourth Amendment and its reasonability determination, Article I, § 7 protections are not 'confined to the subjective privacy expectations of modern citizens.'"[289] The Fourth Amendment is merely a baseline. States can amend their constitutions to make them more protective in these situations by instituting similar language, and courts can regulate the flow of information between individuals and the state.[290] While it is unlikely to occur, legislatures through legislative reform or citizens through ballot initiative may also directly amend their constitutions in order to achieve a narrower application of the search-and-seizure provision in the context of new technology by protecting private affairs more broadly and explicitly stating privacy is protected.[291] Connecticut, Illinois, Washington, and New Mexico are just a few examples of several states that already provide more protection for individual privacy.[292]

These proactive state measures are needed to offset the sole remedy for a Fourth Amendment violation, which is the

---

288 *Id.* at 585.

289 *Id.* (citing State v. Myrick, 688 P.2d 151, 154 (Wash. 1984)).

290 *See* Fakhoury & Kyylai, *supra* note 43. *See also* Eisfeldt, 185 P.3d at 585

> (We have repeatedly held the privacy protected by article I, section 7 survived where the reasonable expectation of privacy under the Fourth Amendment was destroyed. For example . . . this court found a warrantless search of an individual's garbage violated article I, section 7, even though 'it may be true an expectation that [others] will not sift through one's garbage is unreasonable. . . .' By contrast, the United States Supreme Court previously held individuals had no reasonable expectation of privacy in their garbage, and therefore there was no protection under the Fourth Amendment.).

291 *See Amending State Constitutions*, BALLOTPEDIA, https://ballotpedia.org/Amending_state_constitutions (last visited Apr. 14, 2016)

> (Eighteen states allow voters the right to amend their constitution through the ballot initiative process. These states are Arizona, Arkansas, California, Colorado, Florida, Illinois, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, North Dakota, Ohio, Oklahoma, Oregon and South Dakota. As a practical matter, it is considered nearly impossible to meet the ballot qualification standards in Illinois, Massachusetts, Mississippi and Oklahoma. In recent years, additional hurdles have also been enacted in Florida, Montana and Nebraska.).

292 *See supra* note 92 and accompanying text.

exclusionary rule.[293] The exclusionary rule is reactive, and it is not effective enough to handle the new privacy concerns involved with new technology. The outcome when the exclusionary rule is used is that a defendant gets everything he desires while the government gets nothing and loses the evidence.[294] This occurs because the evidence collected becomes entirely inadmissible, and, in most cases, is the only evidence available of the crime.[295] It is a struggle to find even ground because either a criminal walks free, constitutional rights are violated, or a criminal is imprisoned. In each case, Americans are collectively worse off in protecting their rights.[296] Proactive measures, such as more specific guidelines for private searches on computers, are a better remedy and should be utilized to protect individual privacy.[297]

While these are solutions that can help on a state level to create a more uniform application of the private-search doctrine in cases involving computers and other technology by explicitly protecting privacy, a decision by the Supreme Court would provide the best uniformity for the American criminal-justice

---

293 *See Evans*, 514 U.S. at 10 (stating the Supreme Court "ha[s] recognized, however, that the Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands").

294 *See Herring*, 555 U.S. at 141 (citing United States v. Leon, 468 U.S. 897, 900–01 (1984)) ("The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free—something that 'offends basic concepts of the criminal justice system.'").

295 *See id.*

296 *See* Stuntz, *supra* note 102, at 444

> (The exclusionary rule generates a lot of litigation—tens of thousands of contested suppression motions each year. That litigation is displacing something else, and the something else may well have more to do with guilt and innocence. That problem is much more serious than the occasional drug dealer whose Fourth Amendment claim is a ticket to get out of jail: the point is that the exclusionary rule skews the many cases in which drug dealers lose, not just the few that they win. The bottom line is not clear. The literature on this subject (on both sides) tends to assume that this is an easy issue, that suppressing illegally seized evidence is either obviously good or obviously bad. In truth, it is neither. The exclusionary rule is, by a wide margin, the best legal tool available for regulating the police. But it distorts the rest of the criminal justice system. Perhaps this argues for keeping the rule, but within fairly narrow bounds—a direction in which the law has been moving for the past two decades.).

297 *See supra* Section I.B.

system as technology continues to develop.[298] It is important to note that although the whole-computer approach to the private-search doctrine and technology could be the simpler and easier approach,[299] law enforcement is capable of and expected to handle more complex constitutional doctrines. Law enforcement should not shirk on constitutional privacy because it becomes more of a burden to protect individual privacy and follow the principles of the Fourth Amendment.[300] Law enforcement is continually faced with a myriad of difficult issues with computer-related crime, but the police can learn how to handle these issues while not overstepping their authority.[301] The narrow application of the private-search doctrine is preferable because it can serve as a check on law enforcement rather than as an impediment in their work.

Overall, states must adopt more protective measures until the Supreme Court provides clear guidance on how to apply the private-search doctrine to computers.[302] Detailed search-and-seizure manuals with specific sections concerning private searches will help train law enforcement and protect traditional notions of privacy.[303] Also, binding rules protecting individual privacy can be made through common-law decisions.[304] Finally, privacy-focused constitutional provisions may also be used to create more protective search-and-seizure law by explicitly protecting private affairs.[305] Since privacy is integral to American society, states must take action to protect individual privacy by narrowly applying the private-search doctrine to computers in this new digital age.[306]

CONCLUSION

298 *See supra* Part II.

299 *See supra* Subsection II.A.2 (emphasizing that the whole-computer approach is a much more simple application of basic search and seizure law. However, the whole-computer approach allows government to conduct an exhaustive search of the individual's whole computer, where too much personal information is at stake, such as location data, bank statements, photographs, and political affiliations. This approach will result in unwarranted intrusions into an individual's life).

300 *See* Holley, *supra* note 22, at 717.

301 *See supra* Section I.B.

302 *See supra* Section I.B.

303 *See supra* Section I.B.

304 *See supra* Section I.B.

305 *See supra* Section I.B.

306 *See supra* Section III.A.

There are numerous complexities caused by Fourth Amendment searches as applied to new technologies, including privacy concerns with computers, cell phones, and even the emerging use of facial-recognition software.[307] The issue involving the application of the private-search doctrine is a continuing concern for government[308] because courts have treated intrusions in the physical world differently from those in the virtual world.[309] There is no bright line separating privacy rights and the proper constitutional boundary of a government search.[310] However, the private-search doctrine does not allow the government to use private individuals to evade the Fourth Amendment.[311]

Going forward, solutions to this dilemma can occur at a state level with specific procedures and language used in police manuals, protective common-law decisions, and state constitutions that craft more protective articles concerning the search-and-seizure requirements and privacy.[312] The virtual file-or-folder-level approach is currently the best solution available to help protect unwarranted intrusions into the personal lives of Americans.[313] A Supreme Court decision regarding this issue is likely and would result in a more uniform system being used in our criminal justice system regarding the private-search doctrine and the invasion of privacy.[314] A changing digital landscape cannot be allowed to erode American freedoms and give the government free reign over Americans and their personal lives.[315]

---

307 *See supra* Subsection III.A.1.
308 *See supra* Part II.
309 *See supra* Section I.A.
310 *See supra* Part II.
311 *See supra* Part III.
312 *See supra* Section III.B.
313 *See supra* Section III.A.
314 *See supra* Part III.
315 *See supra* Part III.