University of Dayton Law Review

Volume 42 | Number 2 Article 6

12-1-2017

The Private Search Doctrine and Electronic Evidence: A New Approach to Tailor the Fourth Amendment Exception in the Context of Personal Computers

Carly M. Sherman
University of Dayton

THE PRIVATE SEARCH DOCTRINE AND ELECTRONIC EVIDENCE: A NEW APPROACH TO TAILOR THE FOURTH AMENDMENT EXCEPTION IN THE CONTEXT OF PERSONAL COMPUTERS

Carly M. Sherman[*]

I. INTRODUCTION 307
II. BACKGROUND 309
A. *The Rise of "Reasonable Expectation of Privacy" Analysis* 309
B. *Origins of the Private Search Doctrine* 311
C. *Application of the Private Search Doctrine to Computers* 313
1. Physical Box Approach 314
2. Virtual File Approach 316
III. ANALYSIS: NEED FOR A NEW APPROACH 318
A. *Physical Box Approach Minimizes Serious Privacy Interests at Stake* 318
B. *Virtual File Approach is too Restrictive on the Ability of Law Enforcement to Use the Private Search Doctrine as an Investigative Tool* 319
C. *Why Not Create a Blanket Warrant Requirement to Search Personal Computers?* 320
D. *A New Solution* 323
1. Is the computer accessible to multiple users? 323
2. Is there password protection on the computer? 325
3. Is there a P2P file-sharing program installed on the computer? 327
E. *Application of the Balancing Test in Practice* 329
IV. CONCLUSION 330

I. INTRODUCTION

As technology continues to evolve, the court system is facing difficulties in determining how to apply statutes originally designed for use in the physical realm to an increasingly virtual world. At the heart of the conflict between law and technology is the clash between citizens' privacy rights and the evidentiary collection needs of law enforcement during criminal investigations. Of special importance is the collection of data from personal computers, which many individuals use for storage of highly sensitive and personal information. The most recent disagreement among federal circuit

[*] Carly Sherman, J.D. Candidate at the University of Dayton School of Law.

courts highlights this topic: how to apply the private search doctrine in the context of electronic data stored on digital media devices and computers. Subject to certain exceptions, any governmental search of property requires a warrant to be issued by a judge before a search can be conducted by law enforcement officials.[1] However, under the private search doctrine, if a private citizen discovers evidence of a crime while inspecting the property of a third party, the private citizen can report the discovery to law enforcement and a law enforcement officer may conduct a warrantless search of the property in question without violating Fourth Amendment search and seizure procedures.[2] The single limit on this search authority is that the subsequent search must stay within the scope of the private search.[3] In cases involving the private search doctrine and physical evidence of a crime, the constitutional zone of the subsequent search by law enforcement is relatively easy to determine; the boundaries of the zone of search become much blurrier when cases involve electronic evidence.[4]

Opinions of commentators about the scope of a proper search of digital evidence when applying the private search doctrine to a computer vary depending on how each commentator conceptualizes a computer hard drive.[5] Professor Orin Kerr of the George Washington University Law School refers to the two dominant perspectives on how to view a computer hard drive as the "physical box" approach and the "virtual file" approach.[6] Proponents of the physical box approach conceptualize a computer's "entire hard drive as a single closed container"; thus, if a private citizen finds evidence of a crime on an individual's computer, law enforcement officials may conduct a warrantless search of the entire hard drive without violating the individual's Fourth Amendment rights.[7] The United States Court of Appeals for the Fifth and Seventh Circuits have adopted this approach when applying the private search doctrine to digital media devices.[8] Conversely, those in favor of the virtual file approach believe that each file or folder found on a computer hard drive should be viewed as a separate container for the purposes of the Fourth Amendment, limiting the scope of a lawful warrantless search by law enforcement to the computer file or image viewed by the private citizen during the initial private search.[9] The United States Court of Appeals for the

---

[1] *See* DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 1 (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (last visited May 1, 2017).

[2] United States. v. Runyan, 275 F.3d 449, 459 (5th Cir. 2001).

[3] *See* United States v. Jacobsen, 466 U.S. 109, 115 (1984).

[4] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554 (2005).

[5] Marc Palumbo, Note, *How Safe is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 989 (2009).

[6] Kerr, *supra* note 4, at 554.

[7] Palumbo, *supra* note 5, at 978.

[8] United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001); Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012).

[9] Palumbo, *supra* note 5, at 978–79.

Sixth Circuit recently held that the virtual file approach is the proper methodology when the private search doctrine is implicated in the context of evidentiary collection of electronic data by law enforcement.[10]

While both sides of the debate offer strong arguments in support of their respective views on the issue, the adoption of a concrete conceptualization of a computer hard drive is not the best solution for determining how to apply the private search doctrine when a private citizen discovers evidence of a crime on another individual's personal computer. A bright-line rule adopting the physical box approach minimizes the privacy interests at stake, and the virtual file approach largely inhibits law enforcement from effectively using the private search doctrine as an investigative tool. Instead of attempting to force a virtual world of electronic data into the strict confines of the physical world of tangible evidence, this Comment proposes applying a factor-based test on a case-by-case basis to decide the degree of the expectation of privacy an individual exhibits in his/her personal computer in order to determine the proper scope of a governmental search conducted subsequent to a private search. If a high expectation of privacy is evident, according to the specific facts of the case, the proper zone of a warrantless search should be limited to the file viewed during the private search. In the alternative, if it is determined that the individual had a relatively low expectation of privacy, the proper zone of a warrantless search should include the entire computer hard drive.

First, this Comment will begin with a history of the origins of the legal determination of what constitutes a "reasonable" expectation of privacy. Second, it will outline the evolution of the private search doctrine. Third, it will examine rationales and public policy considerations behind the decisions of the Fifth and Seventh Circuits adopting the physical box approach to applying the private search doctrine to digital media devices, and the recent Sixth Circuit decision supporting the virtual file approach. Finally, this Comment will introduce a new resolution to the question of how to apply the private search doctrine in the context of personal computers by proposing the application of a factor-based test to determine on a case-by-case basis the appropriate zone of a warrantless governmental search.

II. BACKGROUND

A. The Rise of "Reasonable Expectation of Privacy" Analysis

The concept that United States citizens are protected from "unreasonable searches and seizures" is embodied in the Fourth Amendment of the Constitution.[11] In the seminal case governing Fourth Amendment

[10] United States v. Lichtenberger, 786 F.3d 478, 488–89 (6th Cir. 2015).
[11] U.S. CONST. amend. IV.

jurisprudence, *Katz v. United States*, the Supreme Court stated the notion that the Fourth Amendment is designed to protect citizens from unreasonable governmental searches and seizures when an individual has a reasonable expectation of privacy in his person and/or property.[12] Charles Katz was convicted of violating a federal statute by transmitting wagering information via telephone.[13] Recordings of incriminating phone calls Katz made from a public phone booth were introduced by the government as key evidence demonstrating Katz's guilt.[14] In order to obtain the recordings, federal agents attached an electronic listening device to the outside of the phone booth, unbeknownst to Katz.[15] Katz appealed his conviction to the Supreme Court, asserting a violation of his Fourth Amendment rights based on the fact that the phone booth was a constitutionally protected area.[16] In response, the government argued that it was not possible to infringe upon a constitutionally protected area without physically entering the space.[17] Dismissing both arguments as misplaced, the Court announced that the Fourth Amendment was enacted with the intention to protect American citizens, not physical areas, against unreasonable searches and seizures and, because Katz had an expectation of privacy in his conversations while using the phone booth, the government violated Katz's privacy rights by recording his oral statements without a warrant.[18] In his concurring opinion, Justice Harlan outlined the two-part test that is still used today to analyze whether an individual has a reasonable expectation of privacy in any given situation: (1) the "person [has] exhibited an actual (subjective) expectation of privacy and, [(2)] that the expectation [is] one that society is prepared to recognize as 'reasonable.'"[19]

Since the Supreme Court decision handed down in *Katz*, the Court has found that an individual may have a reasonable expectation of privacy in a multitude of items, ranging from a reasonable privacy interest in closed containers[20] to a reasonable privacy interest in the interior heat of one's home.[21] Thus, it is not a surprise that it is almost universally recognized that citizens have a reasonable expectation of privacy in the personal computers they own and that government officials are generally required to obtain a search warrant before searching a citizen's personal computer.[22] However, computers are susceptible to the same exceptions to the Fourth Amendment search warrant requirement that apply to any other item in which an individual has a reasonable privacy interest. One such exception is the private search

[12] 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[13] *Id.* at 348.
[14] *Id.*
[15] *Id.*
[16] *Id.* at 351.
[17] *Id.* at 349.
[18] *Id.* at 353.
[19] *Id.* at 361 (Harlan, J., concurring).
[20] United States v. Ross, 456 U.S. 798, 822 (1982).
[21] *See* Kyllo v. United States, 533 U.S. 27, 34–35, 38 (2001).
[22] DEP'T OF JUSTICE., *supra* note 1, at 5.

doctrine.[23]

B. Origins of the Private Search Doctrine

Under the private search doctrine, an individual loses the Fourth Amendment shield against governmental search and seizure of an item when a private citizen has previously searched the item, regardless of whether the private search was reasonable or unreasonable.[24] In light of the "reasonable expectation of privacy" test, the Supreme Court has stated that the rationale behind the doctrine is that any privacy interest in an item searched by a private citizen has been extinguished by the initial search; therefore, a subsequent search by the government does not implicate the Fourth Amendment.[25]

The heart of the private search doctrine was first introduced by the Supreme Court in 1921 when the Court declared in *Burdeau v. McDowell* that there is no Fourth Amendment protection for an invasion of privacy perpetrated by a private party acting without any government involvement.[26] McDowell was a director in a company managed by Henry L. Doherty & Co. of New York, who was later discharged by Doherty & Co. "for alleged unlawful and fraudulent conduct in the course of the business."[27] After McDowell's termination, an officer of Doherty & Co. seized control of McDowell's private office and a large amount of incriminating papers were removed from locked desk drawers and a locked safe.[28] The papers were eventually handed over by Doherty & Co. to the Department of Justice, and—upon learning of the intention of the Special Assistant to the Attorney General of the United States to use the papers as evidence to prosecute McDowell for mail fraud—McDowell filed a petition with the United States District Court for the Western District of Pennsylvania requesting an order that the papers be returned to him.[29] The district court granted McDowell's request and the case was appealed to the Supreme Court.[30] The Supreme Court reversed the lower court's ruling, stating that, if the government comes into possession of incriminating evidence by way of a private search, the government may lawfully retain possession of the evidence and use it to prove an individual's participation in a crime without the need to obtain a warrant for purposes of search and seizure of the evidence.[31]

Almost sixty years later, the Supreme Court formally expressed the

---

[23] *See* Priscilla Grantham Adams, *Fourth Amendment Applicability: Private Searches*, NAT'L CTR. FOR JUST. AND RULE L. (2008), http://www.olemiss.edu/depts/ncjrl/pdf/PrivateSearchDoctrine.pdf (last visited May 1, 2017).

[24] United States v. Jacobsen, 466 U.S. 109, 115, 117 (1984).

[25] *Id.*; Grantham Adams, *supra* note 23, at 1–2.

[26] *See* 256 U.S. 465, 475 (1921).

[27] *Id.* at 472–73.

[28] *Id.* at 473.

[29] *Id.* at 470.

[30] *Id.* at 472.

[31] *See id.* at 476.

private search doctrine as an exception to Fourth Amendment search and seizure requirements, as well as placed limits on its application, in *Walter v. United States*.[32] In *Walter*, the defendants were convicted on charges of interstate transportation of obscene films.[33] The films were discovered when the packages they were contained in were mistakenly shipped to an unintended recipient-company.[34] Employees of the company opened the packages and attempted to view the films, but were unsuccessful.[35] Due to the "suggestive drawings" and "explicit descriptions" attached to the films, suggesting their unlawful nature, the employees contacted federal agents to take possession of the evidence.[36] Upon seizing the packages, the agents viewed the films (without obtaining a warrant) and used the films as evidence to convict the defendants.[37] On appeal, the Supreme Court ruled that the private search doctrine was not a defense to the government's invasion of the defendants' privacy interest in the films because the government had exceeded "the scope of the private search."[38] Although the federal agents had lawfully seized the property from the private citizen-employees, the act of viewing the films constituted an unreasonable search, outside of the scope of the private search, because the employees had not previously viewed the films themselves.[39]

Clarification on how to keep a government search within the scope of a private search was given in *United States v. Jacobsen* when the Supreme Court ruled that a warrantless government search is within the scope of a private search, and thus constitutional, if the subsequent government search does not reveal information that was not previously discovered by the private search.[40] In *Jacobsen*, a package being transported by freight carrier was damaged by a forklift during transport.[41] Following company policy, the employees opened the damaged package, exposing several Ziploc bags containing "a white powdery substance."[42] The employees replaced the Ziploc bags in the package and contacted Federal Drug Enforcement Administration agents.[43] The agents re-opened the package, removed the Ziploc bags, and confirmed the substance within the bags was cocaine.[44] The evidence was used to convict the owners of the package of possession of drugs with intent to distribute and the defendants appealed their convictions to the

---

[32] *See* 447 U.S. 649, 657 (1980).
[33] *Id.* at 651–52.
[34] *Id.* at 651.
[35] *Id.* at 651–52.
[36] *Id.* at 652.
[37] *Id.*
[38] *Id.* at 657.
[39] *Id.*
[40] 466 U.S. 109, 120 (1984).
[41] *Id.* at 111.
[42] *Id.*
[43] *Id.*
[44] *Id.* at 111–12.

Supreme Court on the basis that the government agents had violated their Fourth Amendment rights by exceeding the scope of the private search.[45] Refining the rule discussed in *Walter*, the Court stated that "[t]he Fourth Amendment is implicated only if the authorities use [the] information with respect to which the expectation of privacy has not already been frustrated" by the private search.[46] Applying this standard to the facts of the case, the Court determined that the agents' conduct in re-opening and exposing the contents of the defendants' package did not exceed the scope of the private search conducted by the freight carrier employees because the agents were virtually certain that the package contained nothing more than what the private searchers had already discovered, and the government search "enabled the agent[s] to learn nothing that had not previously been learned during the private search."[47]

Following the Supreme Court decision in *Jacobsen*, a government official conducting a warrantless search subsequent to a private search can be assured that evidence collected will be admissible at trial so long as he/she stays within the scope of the prior search and discovery.[48]

C. *Application of the Private Search Doctrine to Computers*

The two perspectives dominating the debate about how to apply the private search doctrine in the context of personal computers have been termed the "physical box" approach and the "virtual file" approach.[49] Proponents of the physical box approach to searching computers believe that a computer's entire hard drive should be conceptualized as a single closed container.[50] Under this approach, if a private citizen conducts a search of any size on the personal computer of a third party, the private citizen has frustrated the third party's privacy interest in the entire hard drive of the computer.[51] Consequently, a secondary government search has virtually no limits; a government official may search the entire contents of the hard drive and use any information discovered without violating the third party's Fourth Amendment rights.[52]

In contrast, the virtual file approach considerably narrows the private search doctrine exception to Fourth Amendment search and seizure requirements. According to this approach, "individual files or folders on a hard drive [should be construed] as separate entities" and, when a private citizen conducts a search on a third party's computer, the third party's privacy

---

[45] *Id.*
[46] *Id.* at 117.
[47] *Id.* at 119–20.
[48] *Id.* at 120.
[49] Palumbo, *supra* note 5, at 978.
[50] *Id.*
[51] Kerr, *supra* note 4, at 554.
[52] *Id.* at 554–55.

interests are frustrated only in regards to the actual files or folders opened and viewed by the private citizen.[53] A government official conducting a warrantless search after a private search must be careful not to open any files or folders not previously viewed during the private search, or the officer runs the risk of violating the third party's Fourth Amendment rights and having any evidence collected during the warrantless search suppressed at trial.[54]

The distinction between the physical box and virtual file methods to applying the private search doctrine to personal computers is significant, given the broad search authority that the physical box approach offers versus the very narrow search authority granted by the virtual file approach. The discrepancy in the amount of warrantless search authority that the two approaches propose is compounded by the serious privacy interests implicated by searching a personal computer, due to the vast amount of sensitive information an individual typically stores on his/her computer. Recently, the divide between advocates for both approaches was represented, and the importance of this issue illuminated, by a split among the federal circuit courts as to how to apply the private search doctrine in cases involving digital media devices containing electronic information.

1. Physical Box Approach

The Fifth Circuit became the first circuit court to apply the private search doctrine in the context of digital media devices by analogizing compact discs (CDs), floppy disks, and zip drives to closed containers in *United States v. Runyan*.[55] In *Runyan*, the Defendant was convicted of four counts related to child pornography based on evidence police obtained through a private search of the Defendant's residence conducted by the Defendant's estranged wife and several of her friends.[56] Originally entering the Defendant's residence with the intent to retrieve personal articles belonging to the Defendant's estranged wife, the group stumbled upon a duffel bag that contained numerous CDs, floppy disks, zip drives, and Polaroid pictures that appeared to depict child pornography.[57] One of the individuals viewed twenty of the CDs and floppy disks, finding clear images of child pornography.[58] All of the digital media devices were turned over to law enforcement authorities and used as evidence during trial to convict the defendant.[59]

On appeal, the Defendant argued that the evidence should have been suppressed based on contentions that law enforcement had exceeded the scope of the private search in two ways: (1) law enforcement officers viewed more

[53] Palumbo, *supra* note 5, at 978–79.
[54] *Id.* at 979; United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001).
[55] *Runyan*, 275 F.3d at 464.
[56] *Id.* at 455.
[57] *Id.* at 453.
[58] *Id.*
[59] *Id.* at 453–55.

of the disks than the private searchers had viewed, and (2) in regards to the disks private searchers did open, officers viewed more files on each disk than the private searchers had viewed.[60] Drawing a parallel between closed containers and each individual disk, the court answered both arguments by analyzing the Supreme Court ruling in *Jacobsen*.[61] The court determined that the *Jacobsen* decision suggested that it is lawful for an officer to open a container not previously opened during a private search without a warrant if the officer is virtually certain about what the contents of the container will be "based on the statements of the private searchers, [his] replication of the private search, and [his] expertise . . . ."[62] The court stated that a defendant's expectation of privacy in the contents of a container can be frustrated if the private search renders the contents of the container obvious, even if not previously viewed.[63] Applying this rule to the facts, the court agreed with the Defendant's first argument that officers exceeded the scope of the private search because they could not be substantially certain about the contents of the disks that had not been opened during the private search.[64] However, the court rejected the Defendant's second argument that officers exceeded the scope of the private search by viewing more files on each disk than the private searchers had opened.[65] The court stated that privacy interests in a container are frustrated when the private searcher initially opens a container; therefore, law enforcement officers did not exceed the scope of the private search of the disks by viewing more files than the private searchers had viewed.[66]

Adopting the physical box approach used by the Fifth Circuit, the Seventh Circuit subsequently held in *Rann v. Atchison* that digital media devices should be conceptualized as closed containers in the context of the private search doctrine.[67] Through the use of digital evidence contained on a digital memory card from a camera and a computer zip drive, the Defendant in Rann was convicted of two counts of criminal sexual assault and one count of possession of child pornography.[68] The digital media devices containing images of child pornography were brought to the attention of police by the Defendant's wife and daughter (who was one of the defendant's victims).[69] On appeal, the Defendant argued the electronic evidence should have been suppressed because the police exceeded the scope of the private search by viewing the images on the memory card and zip drive, due to the fact that nothing in the court record indicated that either the Defendant's wife or

---

[60] *Id.* at 464.
[61] *Id.* at 463–64.
[62] *Id.* at 463; *see* United States v. Jacobsen, 466 U.S. 109, 119–20 (1984).
[63] *Runyan*, 275 F.3d at 464.
[64] *Id.* at 463–64.
[65] *Id.* at 464.
[66] *Id.*
[67] 689 F.3d 832, 837 (7th Cir. 2012).
[68] *Id.* at 834.
[69] *Id.*

daughter had actually viewed the images on the devices.[70] The Court referenced the Fifth Circuit's analysis of the similar issue in *Runyan* and ruled that digital media devices should be analogized to closed containers for the purpose of private search doctrine analysis.[71] The private searchers stated their knowledge to police that the devices they brought to the police station contained images of child pornography; thus, the Court found the officers did not exceed the scope of the prior search by viewing the images because they could be practically certain about what the stored contents of the devices would be.[72]

Runyan and *Rann* stand for the proposition that electronic storage devices can be analogized to physical containers, and the rules the Supreme Court has developed to govern the private search doctrine application to the collection of evidence from closed containers should be implemented in the context of digital evidence collection from electronic devices.

2. Virtual File Approach

The Sixth Circuit became the third federal appellate court to weigh in on the issue of the private search doctrine application to digital media devices, creating the current circuit split by adopting the virtual file approach in *United States v. Lichtenberger*.[73] In *Lichtenberger*, the Defendant was charged with possession of child pornography based on evidence found by the Defendant's girlfriend during a private search of his personal laptop.[74] The Defendant's girlfriend bypassed the password protection on the laptop and proceeded to open various file folders and click through images they contained, uncovering images of child pornography.[75] After reporting the discovery to the police department, an officer came to the residence the Defendant shared with his girlfriend and she showed the officer several images of child pornography located in multiple folders on the computer.[76] Upon confirmation of the girlfriend's allegations, charges were instituted against the Defendant.[77]

At a pretrial evidentiary hearing, the Defendant's girlfriend testified to seeing about 100 images of child pornography during her initial private search, but that she was unsure if the images later shown to the officer were among the images she had discovered during the original search of the laptop.[78] The Defendant ultimately moved to suppress the evidence during

[70] *Id.* at 835–36.
[71] *Id.* at 837.
[72] *Id.* at 838.
[73] 786 F.3d 478, 488 (6th Cir. 2015).
[74] *Id.* at 480.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.* at 481.

the officer's warrantless search of the laptop.[79] The district court granted the motion to suppress the evidence and the government appealed to the Sixth Circuit, arguing that the evidence was admissible on the grounds that the officer's warrantless search was constitutional under the private search doctrine.[80] In its analysis, the Sixth Circuit rejected the analogy relied upon by the Fifth and Seventh Circuits that a digital media device should be conceptualized as a closed container, stating that one cannot compare the search of a computer to that of a closed container because of the large difference in information storage capacity of the two items.[81] The court went on to say that the massive amount of data stored on a computer makes it impossible to validate a private search based on the "virtual certainty" standard discussed in the Supreme Court decision in *Jacobsen*.[82] The court ruled that, absent virtual certainty on the part of the officer that the only thing he would discover on the laptop would be evidence of the crime alleged by the private searcher, the warrantless search could only comply with the Supreme Court precedent set in *Jacobsen* if the search "enabled the agent to learn nothing that had not previously been learned during the private search."[83] The Sixth Circuit rationalized that the only way the warrantless search at issue could be validated under the private search doctrine is if it was proven that the officer viewed only specific files that were viewed during the private search, thereby only learning information previously learned by the private searcher.[84] Therefore, the Sixth Circuit effectively adopted the virtual file approach.[85] Given the fact that the private searcher in this case testified to being uncertain if she had previously viewed the images that she subsequently showed to the officer, the court stated "there was a very real possibility" that the officer's warrantless search exceeded the scope of the private search and held that the evidence was properly suppressed.[86]

The *Lichtenberger* court advanced the rationale that the inherent differences in the data storage capacity of physical containers and computers cause it to be impossible to use the same method of determining the proper zone of a warrantless government search of a closed container to define limits on the zone of search of a computer hard drive.[87]

---

[79] *Id.*

[80] *Id.*

[81] *Id.* at 488–89.

[82] *Id.* at 488; United States v. Jacobsen, 466 U.S. 109, 119–20 (1984) (holding that a warrantless government search of a container does not exceed the scope of a private search when the government officers are virtually certain that a container holds nothing more than what the private searchers have already discovered, and the warrantless search "enabled the agent to learn nothing that had not previously been learned during the private search").

[83] *Lichtenberger*, 786 F.3d at 488; *Jacobsen*, 466 U.S. at 120.

[84] *See Lichtenberger*, 786 F.3d at 488.

[85] *See id.*

[86] *Id.* at 488–489.

[87] *See id.* at 488.

III. ANALYSIS: NEED FOR A NEW APPROACH

A. Physical Box Approach Minimizes Serious Privacy Interests at Stake

The *Runyan* court outlined the predominant public policy arguments for using the physical box approach when determining the proper zone of search of a personal computer after a private search has previously been conducted.[88] Primarily, if police exceeded the scope of a private search every time they stumbled upon a file or image that the private searcher did not view, it could hinder investigations by inhibiting police searchers out of fear that they may uncover "important evidence that the private searchers did not happen to see and that would then be subject to suppression."[89] If police were deterred from using the private search doctrine due to this likelihood of exceeding the scope of the private search, it would effectively render the private search doctrine obsolete as an investigative tool in the context of digital evidence.[90]

However, proponents of the physical box approach fail to take into account the immense privacy interests at stake by stating that in all private search doctrine cases an individual's privacy interest in every item on his/her personal computer is frustrated simply because a third party happened to view a single file located on the computer. Modern computers are used for a wide variety of purposes, "such as 'postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.'"[91] Exacerbating the privacy interest concern attached to searching personal computer data is the vast amount of information that a modern computer is capable of storing. Data storage in computer hard drives can be broken down into data storage increments referred to as "gigabytes"; a computer with a storage capacity of 200 gigabytes can hold data that amounts to approximately fifteen million physical pages of information[92] and a computer with a storage capacity of 250 gigabytes "can hold more than 30,000 average size photos or songs."[93] Given the sensitive nature of information individuals generally store on their computers, coupled with the extensive information storage capacity of a modern computer hard drive, the physical box approach to the application of

---

[88] United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001).

[89] *Id.*

[90] *Id.*

[91] DEP'T OF JUSTICE, *supra* note 1, at 87 (citing United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007)).

[92] Scott Aurnou, *Computer Basics: How is Electronic Data Stored on a Computer or Mobile Device?*, THE SEC ADVOC. (June 10, 2013), http://www.thesecurityadvocate.com/2013/06/10/computer-basics-how-is-electronic-data-stored-on-a-computer-or-mobile-device/ (last visited May 1, 2017).

[93] Kim Komando, *How Much Computer Storage Do You Really Need?*, USA TODAY (Nov. 30, 2012, 12:03 PM), http://www.usatoday.com/story/tech/columnist/komando/2012/11/30/komando-computer-storage/1726835/ (last visited May 1, 2017).

the private search doctrine is far too broad and violative of privacy interests to be implemented as a bright-line rule in every private search doctrine case involving searches of personal computers.

B. Virtual File Approach is too Restrictive on the Ability of Law Enforcement to Use the Private Search Doctrine as an Investigative Tool

The *Lichtenberger* court discussed the public policy rationale behind the virtual file approach to applying the private search doctrine to personal computers by factoring into its analysis "the strong privacy interests at stake" when searching an individual's personal computer.[94] The court highlighted privacy concerns by noting that most people store very sensitive information on personal computers and it is impossible for an officer to conduct a search of a computer with virtual certainty that the computer only holds information relating to the incriminating evidence uncovered by the private search.[95] From the perspective of a proponent for the virtual file approach, the benefits of granting expansive reign to officers to conduct warrantless searches of personal computer hard drives are outweighed by the risks of infringing the massive privacy interests implicated.[96]

While privacy interests involved in conducting searches of personal computers are a concern used to invalidate the overly broad physical box approach to the application of the private search doctrine to computers, the virtual file approach fails to strike the proper balance between respecting an individual's privacy rights and allowing law enforcement to use the private search doctrine effectively as an investigative tool. Recognizing the vast amount of files that can be stored on a computer hard drive, it is impractical to create a rule where every subsequent search to a private search must exactly replicate the private search in order to find a single incriminating file originally discovered by the private searcher. One reason for the impracticality of this narrow approach is that often private searchers simply stumble upon evidence of a crime on a third party's computer and may forget exactly how they found the incriminating file. Similarly, if more than one file containing evidence of a crime was opened, the private searcher may be uncertain if the files later shown to police were among the group of files viewed during the private search.[97] This type of uncertainty can lead to the suppression of incriminating evidence obtained from the personal computer.[98] Even in the absence of explicit witness testimony that the private searcher is unsure of whether the exact files accessed during the private search were the

---

[94] United States v. Lichtenberger, 786 F.3d 478, 491 (6th Cir. 2015).

[95] *Id.* at 488.

[96] *See id.* at 487.

[97] *See id.* at 481. The defendant's girlfriend uncovered images of child pornography on defendant's laptop during a private search, later testifying to being uncertain if the images she showed to a police officer during a warrantless search had been viewed during the original search. *Id.*

[98] *See id.* at 491.

only files accessed in the secondary government search, it would be relatively easy for defense counsel to raise this doubt in the mind of a judge at a suppression hearing by noting the difficulties involved with duplicating every step involved in the private search.

A second reason for the impracticality of implementing the virtual file approach is the relative ease with which individuals can hide files on their computers by changing the file extension.[99] File extensions appear at the end of a file name and denote the type of information the file contains; for example, an image would typically save with the extension ".jpg," whereas a textual file would generally save with the extension ".doc."[100] An individual hiding an incriminating image on his/her computer can change the file extension from ".jpg" into ".doc," and "[a] search for picture files based on the logical file extensions will no longer locate the file."[101] Thus, without the ability to conduct a search that would typically find the file viewed during the private search, law enforcement and private searchers could be completely reliant on the private searcher's memory of how to find the file location in order to satisfy the rigid requirements the virtual file approach imposes on the private search doctrine.

Due to the difficulty of duplicating a private search, along with the possibility of having incriminating evidence discovered on a defendant's computer suppressed if the warrantless search is not exactly duplicative of the private search, law enforcement officers would largely be deterred from using the private search doctrine as an investigative tool in the context of personal computers if the virtual file approach was adopted.

C. Why Not Create a Blanket Warrant Requirement to Search Personal Computers?

The disagreement over how to apply the private search doctrine to personal computers and the drawbacks to implementing either of the predominant approaches to the matter may cause one to wonder why search warrants are not always required prior to the search and seizure of a personal computer by law enforcement officers. This seems like a fair solution on its face; however, investigations involving personal computers would be greatly hindered if a bright-line rule was created requiring a search warrant in all circumstances in order to search a personal computer, and any privacy interest protected by this alternative suggestion is outweighed by the impediment for law enforcement to pursue the governmental interest in preventing crime.

As an initial matter, it is difficult to meet statutory warrant requirements when attempting to obtain a search warrant for a computer.

---

[99] Kerr, *supra* note 4, at 545.
[100] *Id.*
[101] *Id.*

Specifically, the particularity requirement presents a problem in the context of digital evidence.[102] The Fourth Amendment particularity requirement for warrants places limits on law enforcement by forcing officers to describe to a judge or magistrate the physical confines of a search before obtaining approval to execute the search.[103] One court may determine that a warrant satisfies the particularity requirement by stating that a search is limited to the entire hard drive of a computer; however, a court more concerned with an individual's privacy interests in a personal computer may require that officers narrow the warrant further to describe particular places on a hard drive that are intended to be searched.[104] This type of specificity presents difficulties for law enforcement because the nature of "digital evidence [is that it] can be located anywhere on a hard drive," and it is impossible to rule out particular areas of a hard drive in the investigation.[105]

Even if a law enforcement officer is able to meet statutory warrant requirements necessary to initially *seize* an individual's personal computer, there are drawbacks to the *search* by computer forensic examiners that follows the execution of the warrant.[106] Upon seizure of a computer, the hard drive is sent to a digital forensics laboratory to be examined by computer forensic specialists, taking "critical parts of criminal investigations out of the hands of [law enforcement officers]."[107] Forensic examiners are detached from the details of the investigation being conducted by the investigating officer or agent and may "overlook relevant information" and "expend resources needlessly" by searching for information that is not useful for the investigation.[108] Additionally, the length of time a computer forensic examination takes to complete is an obstacle to effective investigations.[109] Digital evidence has become very important to investigations as technology has continued to evolve. Individuals are increasingly using their personal computers to participate in criminal activities, causing a backlog of cases in digital forensic labs from law enforcement agencies that ranges from weeks to months from the time a computer actually reaches the lab.[110] Often, "[b]y the time computers are examined, it is . . . too late to follow many of the leads that are produced" by the evidence obtained.[111] Aggravating the issue of the backlog of computer forensic examinations is the "emerging trend among the

---

[102] *Id.* at 568.
[103] *Id.*
[104] *Id.* at 569.
[105] *Id.*
[106] Hans Henseler, *Breaking the Backlog of Digital Forensic Evidence*, EVIDENCE TECH. MAG., http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1661 (last visited May 1, 2017).
[107] *Id.*
[108] Charles L. Cohen, *Growing Challenge of Computer Forensics*, THE POLICE CHIEF 74.3 (NOV. 16, 2015, 3:04 PM), http://www.policechiefmagazine.org/growing-challenge-of-computer-forensics/ (last visited May 1, 2017).
[109] *Id.*
[110] Henseler, *supra* note 105.
[111] Cohen, *supra* note 106.

judiciary to set deadlines for the examination of seized material," especially when the material is a personal computer the individual uses for business or personal financial purposes.[112] Thus, a proper search and seizure of a personal computer could be executed, but law enforcement may be judicially compelled to return the device to its owner before an examination of the evidence can be conducted.

Finally, a warrant to search a personal computer may be obtained and evidence may be collected, but, at the trial stage, search warrants for digital evidence collected from computers are easily attacked by defense counsel. Due to the difficulty of satisfying the particularity requirement, defense counsel often attempt to invalidate a search based on improperly exceeding the scope of the search described in the warrant.[113] It can be argued that law enforcement exceeded the scope of the search by either searching in areas that were not described in the warrant or by searching information that was not described in the warrant.[114] The unique nature of searching virtual evidence makes it highly likely that law enforcement officers will exceed the scope of the warrant by searching more files in a hard drive than those described in a warrant or by viewing more information than that which was set forth in the warrant as being sought through the execution of the search.[115] The fact that individuals use personal computers for so many varied uses commingles information in the computer, causing it to be difficult to stay within the parameters of a search warrant, which makes it possible for defense counsel to argue that officers exceeded the scope of the private search and ultimately prevail on a motion to suppress any evidence obtained.[116]

The issues faced when attempting to tailor search warrant requirements originally designed for physical evidence to the search and seizure of electronic data—coupled with limits on the effectiveness of an investigation when computer evidence seized under a warrant is sent to a forensic lab for examination—demonstrate that making a bright-line rule requiring law enforcement officers to always obtain a search warrant prior to searching personal computers would greatly hinder investigations. As a highly useful evidentiary collection tool for law enforcement, the private search doctrine is an important exception to the Fourth Amendment warrant requirement that should not be disposed of in the context of searches of personal computers, which modern criminals are increasingly using as instrumentalities for the commission of their crimes.

---

[112] *Id.*

[113] James Adams, *Suppressing Evidence Gained by Government Surveillance of Computers*, 19 CRIM. JUST. MAG. 1 (2004), http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_surveillance.htm (last visited May 1, 2017).

[114] *See* DEP'T OF JUSTICE, *supra* note 1, at 96–97.

[115] *Id.*

[116] *Id.* at 87, 96.

D. A New Solution

This Comment proposes a new solution to the determination of the proper scope of a government search after a private search has uncovered evidence of a crime on a third party's personal computer: a multi-factor balancing test a judge will implement at the evidentiary hearing prior to trial in order to decide whether the third party exhibited a high or low expectation of privacy in the contents of the information stored on his/her computer. The test will consist of three factors: (1) whether the computer is used by, or accessible to, multiple users, (2) whether access to the computer is password protected and/or the files on the computer are encrypted, and (3) whether there is a peer-to-peer file sharing program installed on the computer. The judge will apply these factors to the facts of the case and determine if the defendant has demonstrated a high expectation of privacy or if the defendant had a low expectation of privacy.

If it is determined that the defendant has exhibited a high expectation of privacy, the virtual file approach will be applied; the warrantless government search must have only revealed the specific files, images, and other data that the private searcher originally uncovered. If the law enforcement officer viewed more files, or different files, during the warrantless search than the private searcher discovered during the private search, the officer will have exceeded the scope of the private search and the evidence collected pursuant to the warrantless search must be excluded.

In contrast, if the judge applies the balancing test to the facts and determines that the defendant exhibited a low expectation of privacy, the physical box approach will be applied; the proper zone of the warrantless government search will be the entire computer hard drive and all criminal evidence collected, whether viewed by the private searcher during the initial search or not, will be admissible at trial.

No one factor in the test will be dispositive; two of the three factors must weigh in favor of a high or low expectation of privacy for the judge to make a determination.

1. Is the computer accessible to multiple users?

The first factor in the balancing test will be whether the personal computer is accessible to multiple people for use and, if so, whether some type of protective measure has been taken to limit the other users' access to the defendant's information stored on the computer.

The United States Court of Appeals for the Third Circuit gave a good example in *United States v. Stabile* of how this factor could be judicially

analyzed.[117] In *Stabile*, the Defendant was convicted of charges related to possession of child pornography using evidence collected during a warrantless government search of the Defendant's computers and accompanying hard drives after the Defendant's live-in girlfriend consented to the search of their home.[118] The Defendant moved to suppress the evidence, causing the court to consider whether the Defendant had a reasonable expectation of privacy in the computer equipment, such that his girlfriend lacked the authority to consent to the search and seizure.[119] The answer to this question turned on whether the Defendant's behavior demonstrated that he had "relinquished his privacy" to files on the computer by allowing others (in this case, his girlfriend) to use the computer and store information on it.[120] Factors the court listed as relevant to the determination included "the identity of the user(s), whether password protection is used, and the location of the computer in the house."[121] Applying the factors to the case, the court concluded that the Defendant had relinquished his expectation of privacy in the computers and hard drives because he failed to use any type of password protection and the computer equipment was "located in common areas of the home, such as on the main floor and in the basement, rather than in a private bedroom."[122] Because the Defendant's girlfriend had unrestricted access to the computer equipment, she had the authority to consent to the warrantless search and seizure.[123]

Performing a similar analysis in the case of *United States v. Burke*, the United States District Court for the Eastern District of California decided whether a defendant had the requisite expectation of privacy to object to the search and seizure of a computer that produced evidence leading to the Defendant's indictment for 33 felony counts relating to bankruptcy and money-laundering.[124] During bankruptcy proceedings instituted against the Defendant, an order was granted for the search and seizure of his property located in a residence in which his wife and daughter lived.[125] The Defendant filed a motion to suppress evidence obtained from his seized computer and, in order to determine whether the Defendant had standing to object to the seizure, the court assessed the expectation of privacy the Defendant had in the computer based on any protective measures the Defendant took to keep his information stored on the computer private from the residents of the home.[126] Because the computer was stored in an office-area that lacked a door or any

[117] *See* 633 F.3d 219, 232–33 (3d Cir. 2011).
[118] *Id.* at 224–25.
[119] *Id.* at 232.
[120] *Id.*
[121] *Id.* (citation omitted).
[122] *Id.* at 233.
[123] *Id.*
[124] No. CR. S-05-0365 FCD, 2009 WL 173829, at *1, *3 (E.D. Cal. Jan. 23, 2009).
[125] *Id.* at *4.
[126] *Id.* at *4–5.

other means of closing the space off from the remainder of the home and the computer "did not require a password to log on," allowing full access to both the Defendant's wife and daughter, the court found that the Defendant had not demonstrated any expectation of privacy in the computer; thus, he was not entitled to object to its search and seizure.[127]

The multi-user accessible factor in the balancing test that this Comment proposes would be analyzed in a very similar way to the analyses of the Third Circuit and district court described above.[128] This factor will weigh against a finding of a high expectation of privacy if the defendant's computer is used by multiple users, or accessible to multiple users, based on its location in a common area of a residence shared by others. A mitigating factor that can increase the expectation of privacy in a personal computer accessible to others will be safeguards such as the requirement of a password to log into the computer or to log into the part of the computer housing the defendant's information, and/or encryption of the defendant's files stored on the computer.[129] "On a multiple-user computer . . . with no arrangements for individual data areas" and no safeguards to restrict other users' access to the defendant's files, the defendant will have a low expectation of privacy in the information stored on the computer.[130]

2. Is there password protection on the computer?

The second factor to be weighed will be whether there is password protection on the computer in the form of a password to log into the computer and access its content and/or encryption of the files located on the computer. General password-protection operates as a "protect[ion] from unauthorized access [to a computer] by requiring users to enter a password before access is allowed."[131]

The United States District Court for the Eastern District of Kentucky has stated that the weakness or strength of a password is irrelevant when deciding if an individual has an expectation of privacy in the information stored on the computer; the mere presence of a password demonstrates that the individual has an expectation of privacy.[132] In *United States v. Wilson*, the Defendant's laptop computer had been discovered in a park and turned over to local police who bypassed the password protection of the laptop in

---

[127] *Id.* at *5.

[128] *See Stabile*, 633 F.3d at 232–33; *Burke*, 2009 WL 173829, at *5.

[129] *See* Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (holding that the Defendant had a reasonable expectation of privacy in password-protected files located on a computer shared with his wife because he kept the password confidential and "affirmatively intended to exclude [his wife] . . . from his personal files").

[130] Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1197 (1995).

[131] Monique C.M. Leahy, *Criminal Trials Involving Password-Protected Evidence*, 117 AM. JUR. TRIALS 193 § 1 (2015).

[132] United States v. Wilson, 984 F. Supp. 2d 676, 685 (E.D. Ky. 2013).

order to search the contents of the computer for information that could help locate the computer's owner.[133] During the search of the computer for clues as to the identity of the owner of the laptop, the police discovered what appeared to be images of child pornography, later used as evidence to charge the Defendant with the crime of possession of child pornography.[134] The Defendant moved to suppress the evidence, alleging the warrantless search violated his Fourth Amendment rights because he had a "constitutionally protected reasonable expectation of privacy in the laptop computer" due to its password protection.[135] The government attempted to prove that the Defendant's password did not show a reasonable expectation of privacy because the password protection feature used by the Defendant came standard on all personal computers and the password was not complex, allowing it to be easily bypassed by law enforcement officers.[136] The district court rejected the government's argument, holding that the "level of password protection used [does not] impact the analysis"; the Defendant clearly demonstrated his expectation of privacy when he used a password, easily bypassed or not, which was intended to keep his information private by excluding access by third parties.[137]

An additional level of password-protection that should be considered when applying this factor to the facts of the case is the presence of data encryption of computer files. Even if a third party can log into an individual's computer, data encryption operates by essentially requiring another password to allow the third party to understand the files on the computer.[138] Encrypted files "appear as scrambled, random nonsense unless [the user] know[s] [the] encryption [password]."[139] Not only do encrypted files appear scrambled to the naked eye, but also to forensic tools; causing the files to be useless in "provid[ing] evidence for law enforcement."[140] Although there have yet to be any court decisions that have meticulously detailed a reasonable expectation of privacy analysis involving computers and the impact of a defendant implementing data encryption to protect computer files, many courts have considered encryption of files to be relevant to the analysis.[141]

---

[133] *Id.* at 679.
[134] *Id.* at 679–80.
[135] *Id.* at 684.
[136] *Id.* at 685.
[137] *Id.*
[138] Chris Hoffman, *Why a Windows Password Doesn't Protect Your Data*, HOW-TO GEEK (Nov. 16, 2015, 3:36 PM), http://www.howtogeek.com/161444/htg-explains-why-a-windows-password-doesnt-protect-your-data/ (last visited May 1, 2017).
[139] *Id.*
[140] Kerr, *supra* note 4, at 546.
[141] *See, e.g.*, United States v. Yudong Zhu, 23 F. Supp. 3d 234, 238 (S.D.N.Y. 2014) (stating the Defendant "exhibited a subjective expectation of privacy in [the contents of his personal laptop] by encrypting the laptop and establishing several layers of passwords . . ."); United States v. Rutherford, No. ACM 36651, 2007 WL2035060, at *3 (A.F. Ct. Crim. App. June 19, 2007) (holding the Defendant did not have a subjective expectation of privacy in e-mails contained on his work computer when the Defendant "was required to pass [the computer] to his successor and the e-mails themselves were not separately

Like the *Wilson* court's analysis of password protection, a judge considering the password protection factor while conducting the balancing test this Comment proposes, in the context of data encryption, should not consider the complexity of a password in its analysis.[142] This factor should weigh in finding a high expectation of privacy if a password is required to log into the defendant's computer, or the area of the computer housing the defendant's files, whether the password would be considered easy or difficult to bypass. However, if the password is not kept confidential, this fact will negate a finding of a high expectation of privacy because a password that is not kept confidential is "almost as ineffective as not having any password[] at all."[143] Additionally, if the defendant's files on the computer are encrypted, this fact should weigh heavily in concluding that the defendant has a high expectation of privacy. Data encryption provides strong protection for files stored on a computer because encrypted files are impossible to decipher unless a user has knowledge of the password required to bypass the encryption.[144] If the defendant has encrypted the files on his/her computer, he/she has clearly shown a high expectation of privacy in the contents of the files. However, the presence of data encryption can be negated, just as the presence of a password, if a third party knows the password to override the encryption, or if the defendant has allowed access by third parties to the files through the use of a peer-to-peer (hereinafter "P2P") file-sharing program installed on the defendant's computer.[145]

3. Is there a P2P file-sharing program installed on the computer?

The final factor in the balancing test will be whether the defendant has a P2P file-sharing program installed on his/her computer. An individual downloads software to install a P2P file sharing program to a personal computer and the program allows the sharing of files via the Internet by connecting the computers of all individuals running the same P2P file sharing software; it is possible for millions of computers to be connected at one time through a P2P file-sharing network.[146] Files can be shared between users'

encrypted or protected to preclude access by someone using that computer"); Miller v. State, 335 S.W.3d 847, 854–855 (Ct. App. Tx. 2011) (holding the Defendant did not demonstrate a subjective expectation of privacy in a thumb drive because he did not take any precautions to protect the data it contained, "such as protecting it with a password, [or] encrypting the data . . ."); State v. Turner, 805 N.E.2d 124, 132 (Ohio Ct. App. 2004) (stating one reason that officers did not violate any expectation of privacy Defendant may have had in statements he made while participating in an online chatroom was that the Defendant did not use any password or encryption protection to maintain his privacy in the chatroom conversation).

[142] *See* United States v. Wilson, 984 F. Supp. 2d 676, 685 (E.D. Ky. 2013).

[143] *Choosing and Protecting Passwords*, US-CERT (May 21, 2009), https://www.us-cert.gov/ncas/tips/ST04-002 (last visited May 1, 2017).

[144] Hoffman, *supra* note 137.

[145] *See* State v. Daigle, 93 So. 3d 657, 665–66 (La. Ct. App. 3d Cir. 2012) (holding that there was not a violation of the Defendant's privacy interest in a warrantless search of encrypted files when the Defendant had freely opted to share the files with others via a P2P file sharing program).

[146] United States v. Stults, 575 F.3d 834, 838 (8th Cir. 2009); FED. TRADE COMM'N, *P2P File-Sharing Risks* (Sept. 2011), https://www.consumer.ftc.gov/articles/0016-p2p-file-sharing-risks (last visited May 1, 2017).

computers intentionally, or "files may be sent from one user's computer to another user's computer without the permission or knowledge of the other user."[147] Users of P2P file-sharing programs open themselves up to the risk that all of the information stored on their computer hard drives could be exposed and accessible to other users.[148]

The United States Court of Appeals for the Eighth Circuit has affirmatively held that an individual cannot have a reasonable expectation of privacy in computer files made accessible to third parties over a P2P file sharing network.[149] In *United States v. Stults*, the Defendant was indicted for possession of child pornography after an agent for the FBI conducted a search for child pornography over a P2P file-sharing network that ultimately led to the discovery of child pornography on the Defendant's computer connected to the network.[150] The Defendant appealed his subsequent conviction for the charges based, in part, on a violation of his Fourth Amendment rights when the government agent conducted a warrantless search of the Defendant's personal computer by accessing the incriminating evidence using the P2P file sharing network.[151] While noting that an individual generally has an expectation of privacy in the contents of his/her personal computer, the court ruled that there was no Fourth Amendment violation in this case because the Defendant eliminated his expectation of privacy when he decided "to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program."[152]

The Ninth Circuit has further held that an individual negates an expectation of privacy in his/her personal computer by installing a P2P file sharing program, regardless of whether the individual actually intended to share files on his/her computer over the file sharing network.[153] The Defendant in *United States v. Borowy* was convicted of possession of child pornography when an FBI agent monitoring child pornography trafficking accessed images of child pornography being shared from the Defendant's computer via a P2P file sharing program installed on the Defendant's computer.[154] The Defendant appealed the conviction, claiming the agent violated his Fourth Amendment rights when he accessed the Defendant's computer files without a warrant.[155] The Defendant argued that, though unsuccessful, he had attempted to customize the settings on the program to prevent other users from downloading the files located on his computer, claiming that his belief that his files were inaccessible to others created

---

[147] *Stults*, 575 F.3d at 838.
[148] FED. TRADE COMM'N, *supra* note 145.
[149] *Stults*, 575 F.3d at 843.
[150] *Id.* at 839.
[151] *Id.* at 837.
[152] *Id.* at 843.
[153] 595 F.3d 1045, 1048 (9th Cir. 2010).
[154] *Id.* at 1046–47.
[155] *Id.* at 1047.

a reasonable expectation of privacy in the files.[156] Dismissing this argument, the court stated that even if the Defendant was unaware his computer files were accessible to others, he had been aware that he had installed "a file-sharing program [designed to] allow the public at large to access files" on his computer.[157] The fact that the files were open to be viewed and shared by the public negated any reasonable expectation of privacy, and the court held the Defendant's Fourth Amendment rights had not been violated by the agent's warrantless search.[158]

The presence of a P2P file-sharing program on a defendant's personal computer should strongly suggest to a judge—who is implementing the balancing test this Comment advances—that the defendant had a low expectation of privacy in the information stored on his/her computer. As the Ninth Circuit has stated, the defendant's subjective intent to share files stored on his/her computer with other users should be irrelevant to the judge's consideration when weighing this factor. The fact the defendant intentionally installed a program onto his/her computer that is designed to grant third party access to view and download files between computers connected to the P2P file-sharing network is enough to contradict a high expectation of privacy in the contents of the computer.[159] "Knowingly placing material into an environment in which third parties can and do routinely access it without restriction is inconsistent with claiming a reasonable expectation of privacy in that material."[160]

E. Application of the Balancing Test in Practice

In order to understand how a judge might conduct the three-factor balancing test this Comment proposes, consider this hypothetical situation: a defendant has been charged with possession of child pornography; the primary evidence for the prosecution is several images of child pornography found on the defendant's laptop computer. While searching the computer hard drive for a certain family photo, the defendant's wife stumbled upon the images of child pornography and immediately called the police. An officer arrived at the home and the defendant's wife showed him the images she had found, constituting a warrantless search of the computer. These images are now before the judge at the pretrial evidentiary hearing for admissibility.

Due to the fact that the private search doctrine has been implicated in the context of a search of computer evidence, the judge must conduct the three-factor balancing test in order to determine the proper scope of the officer's warrantless search and, consequently, if the officer stayed within the confines of the zone of proper search.

---

[156] *Id.*
[157] *Id.* at 1048.
[158] *Id.*
[159] *See id.*
[160] 1 INFORMATION LAW § 8:5, Westlaw (database updated Nov. 2015).

In regards to the first factor, the laptop computer is a multi-user computer; it is used by both the defendant and his wife, and the computer is always left in the family room of the couple's home (a common area). This factor weighs in favor of finding a low expectation of privacy.

The second factor requires the judge to look at the password protection on the computer. The computer has a password to log onto the home screen and, once on the home screen, both the defendant and wife have separate passwords to log into specific folders housing their personal files. Although the defendant's wife discovered at some point in the marriage that the defendant uses the couple's anniversary date for all of his passwords (which ultimately allowed her access to his files located on the computer), the fact that the defendant has a password that is intended to exclude third parties, including his wife, from access to the information he stores on the computer weighs in favor of finding a high expectation of privacy.

The third factor is easy for the judge to decide; the couple does not have a P2P file sharing program installed on the laptop. Now the judge must weigh the factors: two out of the three factors weigh in favor of finding a high expectation of privacy, thus, the proper zone of search for the warrantless government search following the private search must be limited only to the images that the defendant's wife viewed during the private search. If the officer viewed any additional images during the warrantless search that the defendant's wife had not viewed during the private search, the officer will have exceeded the scope of the private search and all evidence collected during the warrantless government search must be excluded.

If the facts of the hypothetical scenario were changed slightly, the judge could have found that the balancing test tipped in favor of finding that the defendant had a low expectation of privacy in the contents of the personal computer. If this was the decision, the proper zone of search for the warrantless government search that followed the private search would be the computer's entire hard drive. Therefore, the officer would not have exceeded the scope of the private searching by viewing any different, or additional, files that the defendant's wife had not viewed during the initial private search and all evidence collected from the computer would be admissible at trial.

IV. CONCLUSION

The law surrounding the application of the private search doctrine to personal computers is uncertain and neither the physical box approach, nor the virtual file approach, present workable solutions to the problem. Computers are increasingly becoming important pieces of evidence during criminal investigations and the Fourth Amendment privacy concerns implicated by this fact require clarity and uniformity in this area of the law. This Comment presents a viable solution to this problem by proposing a

balancing test that can be implemented by judges during evidentiary hearings in order to determine the proper zone of a warrantless government search subsequent to a private search. Although it is possible that a balancing test may be met with opposition from the judiciary and law enforcement, the test has clear guidelines and could be conducted relatively quickly and easily. Judges frequently use balancing tests to make legal determinations on a case-by-case basis and the factors involved in this particular balancing test create a concise checklist for an officer to use to assess the circumstances before conducting a warrantless search subsequent to a private search in order to make a preliminary determination of the proper zone of search. This three-factor balancing test offers a fair resolution for the battle between the societal interests in protecting personal privacy and thwarting crime with effective government investigations.