ATTACHMENT A

[J-107-2018]
IN THE SUPREME COURT OF PENNSYLVANIA
WESTERN DISTRICT

SAYLOR, C.J., BAER, TODD, DONOHUE, DOUGHERTY, WECHT, MUNDY, JJ.

COMMONWEALTH OF PENNSYLVANIA,	:	No. 16 WAP 2018
	:	
Appellee	:	Appeal from the Order of the Superior
	:	Court entered December 21, 2017 at
	:	No. 435 WDA 2017, affirming the
v.	:	Judgment of Sentence of the Court of
	:	Common Pleas of Butler County
	:	entered March 9, 2017, at No. CP-10-
JON ERIC SHAFFER,	:	CR-0000896-2016.
	:	
Appellant	:	ARGUED: December 6, 2018

OPINION

JUSTICE BAER **DECIDED: JUNE 18, 2019**

This is an appeal from the judgment of the Superior Court, which affirmed the trial court's order denying a motion to suppress images of child pornography discovered by a computer repair shop employee after Jon Eric Shaffer ("Appellant") took his laptop to the commercial establishment for repair and consented to the replacement of the laptop's hard drive. The Superior Court held that the trial court did not err in denying suppression because Appellant abandoned his reasonable expectation of privacy in the computer files under the facts presented. We affirm the judgment of the Superior Court, albeit on different grounds. *See Commonwealth v. Wholaver*, 177 A.3d 136, 145 (Pa. 2018) (holding that this Court may affirm a valid judgment or order for any reason appearing of record).

We hold that because the contraband images were discovered by a computer technician who was not acting as an agent of the government and because the police

officer's subsequent viewing of the contraband images did not exceed the scope of the computer technician's search, the private search doctrine applies and Appellant's constitutional privacy protections are not implicated.[1]

I. Background

The facts of this case, as revealed during the suppression hearing, are as follows. On November 25, 2015, Appellant delivered his laptop computer to CompuGig, a computer repair shop. To obtain repair services, Appellant was required to complete CompuGig's intake form, which queried "What problems are you experiencing?" and listed several alternatives. Commonwealth Exhibit 1. Appellant marked the boxes indicating "Spyware/virus" and "Can't get to Internet." *Id.* He also provided his computer login password. *Id.* Additionally, CompuGig's administrative log indicated that Appellant informed a CompuGig employee that his "son downloaded some things and now there are a lot of pop-ups. Internet has stopped working." Commonwealth Exhibit 2, at 1.

After conducting diagnostic testing, CompuGig technician Justin Eidenmiller believed that Appellant's computer had a failing hard drive. Consistent with CompuGig's policy of contacting the customer for approval if the service charges will exceed $160, an administrative employee called Appellant on December 4, 2015, and Appellant consented to the replacement of the hard drive.[2] In an effort to replace the hard drive, Eidenmiller

---

[1] As discussed in detail, *infra*, the High Court in *United States v. Jacobson*, 466 U.S. 109 (1984), held that a search conducted by private citizens is not protected by the Fourth Amendment. Any additional invasion of privacy by the government must be examined by considering the degree to which the government exceeded the private search. *Id.* at 115. This Court has acknowledged this rule of law in relation to both the federal and state constitutions. *See Commonwealth v. Harris*, 817 A.2d 1033, 1047 (Pa. 2002) (recognizing that "[t]he proscriptions of the Fourth Amendment and Article I, Section 8 do not apply to searches and seizures conducted by private individuals").

[2] The exact contents of this conversation are unknown as the administrative employee who called Appellant did not testify at the suppression hearing. The record establishes,

attempted to "take an image of the hard drive and put it on a new hard drive at the customer's request." N.T., 7/7/2016, at 6. While Eidenmiller obtained an image of the hard drive, he was unable to transfer that image successfully to a new hard drive.[3] *Id.*

The next day, after several unsuccessful attempts to transfer files from the hard drive, Eidenmiller continued his efforts to relocate the contents of the hard drive to the new hard drive by manually opening each individual folder and copying the contents. *Id.* at 7. During this process, Eidenmiller observed thumbnail images, *i.e.*, small images reflecting the identify of a computer file's contents, revealing what he believed to be sexually explicit photos of children. *Id.* at 7, 23-24. Notably, Eidenmiller had not been searching for that kind of information and had never been asked by law enforcement to keep watch for evidence of child pornography. *Id.* at 7, 13. Eidenmiller informed his boss of the images he discovered, and an administrative employee of CompuGig contacted the police. *Id.* at 7.

Later that afternoon, Officer Christopher Maloney of the Cranberry Township Police Department arrived at CompuGig. The store owners advised Officer Maloney that technicians had found explicit images of young girls on Appellant's laptop and took the officer to the room where Eidenmiller had been working on the computer. *Id.* at 28.

---

however, that Eidenmiller was told by CompuGig administration to continue working on the laptop because Appellant had consented to replacing the hard drive. Notes of Testimony ("N.T."), Suppression Hearing, 7/7/2016, at 17-18. Further, CompuGig's log indicated "Called customer to explain that we must do an OS Rebuild with data." Commonwealth Exhibit 2, at 2.

[3] CompuGig's administrative log indicated a second communication between Appellant and CompuGig when, on November 30, 2015, Appellant had called CompuGig, purportedly to check on the status of his repair, and was given a quote of $250.50 to cover "New 500 Gig HDD," "Reinstall image," and "PE." Commonwealth Exhibit 2, at 3. The log further indicated that Appellant was in a rush to have the repair completed as he used the laptop for his business. *Id.*

Officer Maloney asked to see the images that Eidenmiller had found. *Id.* at 28-29. Eidenmiller complied and showed Officer Maloney the child pornography images he had discovered, using the "exact route taken to find the images." *Id.* at 9, 30.[4] Germane to this appeal, after viewing the images that Eidenmiller displayed, Officer Maloney directed Eidenmiller to "shut down the file" and seized the laptop, external hard drive copy, and power cord. *Id.* at 29.

On December 11, 2015, Detective Matthew Irvin of the Cranberry Township Police Department went to Appellant's home and questioned him. Appellant admitted to having some images on his computer depicting children as young as eight years old in sexually explicit positions and identified the folders where the digital images were stored. Detective Irvin thereafter obtained a search warrant for the laptop and accompanying hardware on December 15, 2015.[5] *Id.* at 31. While the suppression record does not indicate when the search warrant was executed, there is no evidence suggesting that police conducted an independent search of the files on Appellant's laptop beyond what was observed at CompuGig prior to obtaining the warrant.

On December 18, 2015, Detective Irvin met with Appellant a second time and obtained a written inculpatory statement regarding the illegal images. The following month, on January 21, 2016, a criminal complaint was filed against Appellant charging him with sexual abuse of children (possession of child pornography), 18 Pa.C.S. § 6312(d), for possessing seventy-two digital images, which depicted a child under eighteen years of age engaging in a prohibited sexual act or in the simulation of such act. The complaint also charged Appellant with criminal use of a communication facility (laptop

[4] The record does not disclose the precise number of images that Eidenmiller found and displayed to Officer Maloney.

[5] Detective Irvin did not testify at the suppression hearing; rather, Officer Maloney testified that Detective Irwin questioned Appellant and subsequently obtained a search warrant.

computer), 18 Pa.C.S. § 7512(a), for utilizing the internet to commit, cause or facilitate the commission of the felony of sexual abuse of children.

On May 27, 2016, Appellant filed a pretrial omnibus motion to suppress the contraband images discovered on the hard drive of his laptop computer. Acknowledging that a CompuGig employee had summoned Officer Maloney to the establishment after discovering the illegal images, in his suppression motion, Appellant asserted that an illegal search occurred at the moment Officer Maloney directed the CompuGig employee to open Appellant's computer files and display the suspected contraband images that Eidenmiller had discovered, after which Officer Maloney viewed the images and seized the laptop and the copy of the external hard drive.[6] Defendant's Omnibus Pretrial Motion, at ¶ 4, 8. Appellant maintained that Officer Maloney's discovery of the evidence was neither inadvertent nor involved exigent circumstances because the CompuGig employee had informed the officer that the illegal images were on the laptop and that the laptop had been secured in the backroom of the CompuGig facility. Under these circumstances, Appellant submitted, Officer Maloney was required to obtain a warrant before conducting a search of his computer files.

Appellant further contended in his suppression motion that this police conduct constituted a warrantless search of his laptop in violation of his reasonable expectation of privacy, as well as a trespass upon his property in violation of Article I, Section 8 of the Pennsylvania Constitution and the Fourth and Fourteenth Amendments to the United States Constitution. *Id.* at ¶ 8.[7] Relevant here, Appellant argued that he did not abandon

---

[6] Appellant did not challenge the chain of custody of his laptop in his suppression motion or suggest that police searched the laptop after seizing it at CompuGig, but before obtaining a warrant.

[7] Appellant did not argue in his suppression motion that Article I, Section 8 offers greater protection than the Fourth Amendment under the circumstances presented.

his expectation of privacy in the files stored on his laptop when he took the computer to CompuGig for repair. He further argued that the incriminating statements he made to police after this illegal search and seizure were the fruit of the unlawful police conduct. *Id.* at ¶ 9. Accordingly, Appellant requested that the trial court suppress the physical evidence seized and all the fruits thereof.

In opposing Appellant's suppression motion, the Commonwealth did not specifically invoke the private search doctrine. Instead, the Commonwealth took the position that once Appellant gave his laptop to CompuGig for repairs, he abandoned his expectation of privacy in the computer files stored on the laptop. In support of this position, the Commonwealth relied upon the Superior Court's decision in *Commonwealth v. Sodomsky*, 939 A.2d 363 (Pa. Super. 2007). As the parties' arguments and the lower courts' decisions revolve around the *Sodomsky* decision, we shall examine that case.

In *Sodomsky*, the defendant went to a Circuit City store and requested the installation of an optical drive and DVD burner onto his desktop computer. The defendant was informed that as part of the installation process, the installer would have to make sure that the DVD burner worked. The defendant did not inquire as to how operability of the DVD burner would be determined. After the software was installed, a computer technician performed a general search of the defendant's computer files for a video to test the new DVD drive. During this general search, the technician observed titles of videos which appeared to be pornographic in nature because their titles included masculine first names, ages of either thirteen or fourteen, and sexual acts. The technician clicked on the first video title that appeared questionable, and the video contained the lower torso of an unclothed male and a hand approaching the male's penis. The technician immediately stopped the video and contacted his manager, who summoned the police.

The police arrived at the Circuit City store and viewed the same video clip discovered by the technician. When the defendant arrived shortly thereafter to retrieve his computer, the police informed him that his computer was being seized because police suspected that it contained child pornography. The defendant responded that he knew what they had found and that "his life was over." *Id.* at 366. Police seized the computer. After obtaining a warrant, the police searched the computer and discovered child pornography. The defendant filed a motion to suppress the illegal images, which the trial court granted. The trial court reasoned that the defendant retained a privacy interest in the computer files as he did not expect the computer's contents to be published to anyone other than Circuit City employees who were performing the requested installation.

On appeal to the Superior Court, the issue was whether the defendant's "expectation of privacy in the videos on the computer that he relinquished to Circuit City employees for repairs was reasonable or whether he knowingly exposed the computer's video files to the public such that he voluntarily abandoned his privacy interest in them." *Id.* at 367. The *Sodomsky* court examined the theory of abandonment in Pennsylvania, acknowledging that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 367 (quoting *Katz v. United States*, 389 U.S. 347, 351-52 (1967)).

Emphasizing that abandonment is a question of intent that is dependent upon the facts and circumstances presented, the *Sodomsky* court concluded that the defendant had no reasonable expectation of privacy in his illegal computer files. First, the court observed that the defendant requested the installation of a DVD drive, that Circuit City employees informed him that the drive's operability would be tested, and that the defendant did not inquire as to the manner of testing or restrict the employees' access to

his computer files. *Sodomsky*, 939 A.2d at 368. The court concluded that the defendant "should have been aware that he faced a risk of exposing the contents of his illegal video files." *Id.*

Although not characterizing the initial search as a private one, the *Sodomsky* court found it critical that when the child pornography was discovered, the computer technicians were testing the "drive's operability in a commercially-accepted manner" and were not searching for contraband. *Id.* The court further emphasized the voluntary nature of the defendant's actions in leaving his computer at the store without deleting the child pornography videos or altering the videos' illicit titles. *Id.* at 369.

The Superior Court distinguished the *Sodomsky* case from *Commonwealth v. DeJohn*, 403 A.2d 1283 (Pa. 1979), where this Court held that a bank could not submit a customer's bank records to the police absent a search warrant because one's disclosure of financial records to a bank was not entirely volitional as one cannot participate in the economic life of contemporary society without a bank account. To the contrary, the court held that the defendant in *Sodomsky* was not compelled to take his computer to Circuit City for repair and could have elected to leave the store with the computer after being informed that the DVD burner's operability would be examined, instead of risking discovery of the illegal images. *Sodomsky,* 939 A.2d at 369. The court concluded that because the defendant abandoned his privacy interest in the child pornography videos on his computer, he could not object to the subsequent viewing of the video list and file by police. *Id.*

Finally, the *Sodomsky* court rejected the defendant's contention that the seizure of the computer was improper absent a warrant. The court held that the plain view exception to the warrant requirement applied because the police had been invited to the repair center in Circuit City, the videos were not obscured and could be readily seen from that

location, the incriminating nature of the video files was immediately apparent based on the graphic titles assigned to the videos, and the police had the lawful right to access the videos because the defendant had abandoned any reasonable expectation of privacy in them.[8] *Id.* at 370.

Returning to the instant case, at the suppression hearing on July 7, 2016, two witnesses, Eidenmiller and Officer Maloney, testified to the aforementioned facts. The parties' arguments focused exclusively upon the applicability of the *Sodomsky* decision. Following the hearing, the trial court denied Appellant's suppression motion, finding that the present facts were similar enough to render *Sodomsky* controlling. Trial Court Opinion, 10/3/2016, at 7. While the trial court did not agree with the Commonwealth that under *Sodomsky* Appellant abandoned his expectation of privacy in his computer files as soon as he delivered the laptop for repair, the court held that Appellant abandoned his expectation of privacy when he requested repairs on his computer related to complaints of a virus and an inability to use the Internet and consented to the replacement of his hard drive.

The trial court found that the instant circumstances would "obviously lead a person to conclude that CompuGig was likely to perform work related to the hard drive and the files contained on it [and that Appellant] was or should have been aware that he faced a risk of exposing the files contained thereon, as was the case in *Sodomsky*." *Id.* at 9. Also similar to *Sodomsky*, the trial court held that when the images of child pornography were discovered, the CompuGig technician was not conducting a search for illicit items, but was attempting to transfer the files from Appellant's hard drive to a new drive. *Id.* The

[8] Judge Colville filed a concurring opinion in which he opined that he would not engage in a plain view analysis as the defendant's challenge fails because he lacked a reasonable expectation of privacy in the videos stored on his computer after he delivered the computer to Circuit City.

court further opined that Appellant's actions in delivering his laptop to CompuGig for repairs and consenting to the replacement of the laptop's hard drive were voluntary and were not required for Appellant to function in society, distinguishing the case from this Court's decision in *DeJohn*. *Id.* at 9-10.

Concluding that Appellant abandoned his privacy interest in the files at issue, the trial court found that he could not object to the subsequent viewing of the files by police as Officer Maloney properly seized the laptop under the plain view exception to the warrant requirement. *Id.* at 10. The court reasoned that Officer Maloney was lawfully at the CompuGig store at the invitation of the store's owners, the computer and files were not obscured and could be plainly seen from that location, the incriminating nature of the files was readily apparent, and Officer Maloney had a lawful right of access to the computer files because Appellant had abandoned his privacy interest in them. *Id.* at 10.

The trial court further rejected Appellant's challenge to the search and seizure of his computer based upon a trespass analysis, concluding that Eidenmiller was engaged in conduct permitted by Appellant when the files were discovered; thus, he was not trespassing on Appellant's effects. *Id.* at 10. Relevant here, the trial court emphasized that Officer Maloney never expanded upon Eidenmiller's actions, but merely viewed the images that Eidenmiller presented to him. *Id.* at 11.

On November 10, 2016, the trial court, sitting as finder of fact, found Appellant guilty of both charges (possession of child pornography and criminal use of a communication facility) and subsequently sentenced him to an aggregate six to twelve months of incarceration, followed by 156 months of probation. Appellant appealed his judgment of sentence to the Superior Court, raising the single issue of whether the trial court erred in failing to suppress evidence from the warrantless search and seizure of his laptop. As it did before the trial court, the Commonwealth again contended that the

Sodomsky decision was controlling, while Appellant maintained that *Sodomsky* was distinguishable or, in the alternative, should be overturned.

The Superior Court affirmed Appellant's judgment of sentence in a published decision. *Commonwealth v. Shaffer*, 177 A.3d 241 (Pa. Super. 2017). Initially, the court declined Appellant's invitation to overrule *Sodomsky,* finding that such action should be taken by either an *en banc* panel of the Superior Court or this Court. *Id.* at 246. Further, the Superior Court was unpersuaded by Appellant's attempt to distinguish *Sodomsky* on the ground that it was unforeseeable that the technician replacing his hard drive would have been unable to take an image of the entire hard drive, causing him to copy Appellant's files manually from the old hard drive to the new one, thereby exposing his illicit photographs.

The court emphasized that in *Sodomsky*, the defendant made a similar contention, alleging that he was unaware that the technician intended to run a test on the new DVD drive using a video from the defendant's hard drive. In both cases, the Superior Court reasoned, the defendants did not inquire as to how the repair procedure would be executed or restrict in any way the computer technician's access to the illegal files. *Id.* The Superior Court further noted that in both cases the computer technicians were completing repairs in a commercially-accepted manner and were not conducting a search for illicit items when they inadvertently discovered the child pornography. *Id.* at 247. The court concluded that any factual distinctions between the two cases favored the denial of suppression in the instant case as Appellant was informed that CompuGig needed to transfer all of his files and the illicit images appeared obviously in thumbnail images when Eidenmiller opened a folder on the hard drive. *Id.* Accordingly, the Superior Court concluded that, like the defendant in *Sodomsky*, Appellant abandoned his expectation of

privacy in the contents of his computer files; thus, the trial court did not err in denying his motion to suppress.

As noted, this Court granted allowance of appeal to determine whether the Superior Court erred in determining that Appellant abandoned his expectation of privacy in child pornography files stored on his computer under the facts presented.

II. The Parties' Arguments

Appellant contends that the trial court erred in denying suppression of the physical evidence obtained from his laptop and his resulting confessions because such evidence was obtained without a warrant or consent and in the absence of exigent circumstances, thereby violating his right against unreasonable searches and seizures under both Article I, Section 8 of the Pennsylvania Constitution and the Fourth Amendment to the United States Constitution.[9,10] Appellant acknowledges that for these constitutional protections to apply, the citizen must first establish a subjective expectation of privacy in the area searched or the effects seized and must demonstrate that the expectation is one that society is prepared to recognize as reasonable. Brief for Appellant, at 9. He posits,

---

[9] The Fourth Amendment to the United States Constitution provides that "[t]he 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." U.S. CONST. amend. IV.

Article I, Section 8 of the Pennsylvania Constitution provides that "[t]he people shall be secure in their persons, houses, papers and possessions from unreasonable searches and 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 subscribed to by the affiant. PA. CONST. art. I, § 8.

[10] Appellant does not contend in his brief to this Court that Article I, Section 8 of the Pennsylvania Constitution offers any greater protection than the Fourth Amendment. Accordingly, we assume for purposes of argument that both provisions offer the same protection under the circumstances presented.

however, that one cannot abandon his reasonable expectation of privacy unless he does so with intent or where it is reasonably foreseeable to him that his actions will relinquish his privacy to others.

Appellant maintains that he did not intend to relinquish his reasonable expectation of privacy in his computer files when he took his laptop to CompuGig for enumerated repairs. Further, he submits, it was not reasonably foreseeable that his private computer files would be accessed by CompuGig employees. Appellant explains that only a "convoluted chain of events" prompted discovery of the illegal images as Eidenmiller determined that his laptop's hard drive was failing, attempted to copy the entire hard drive to a new drive using particular software, and was ultimately forced to copy folders onto the new hard drive manually. Brief for Appellant, at 10. He asserts that it was not until Eidenmiller was unable to copy some of the folders that the individual files were opened for copying purposes, thereby revealing the contraband images.

Appellant contends that if this scenario is interpreted as being reasonably foreseeable, he cannot imagine an instance where one would retain a reasonable expectation of privacy in his computer files when the computer is taken to a commercial establishment for repair. Emphasizing one's general inability to repair a broken computer, Appellant likens his case to *Commonwealth v. DeJohn, supra*, where this Court held that one does not lose his reasonable expectation of privacy when he discloses financial records to his bank because disclosure of these records is not entirely volitional, considering that one cannot participate in the economic life of contemporary society without a bank account. He asserts that the same is true for personal computers.

Regarding the application of the Superior Court's decision in *Sodomsky*, Appellant neither expressly requests that we overrule that decision nor distinguishes that case from the facts presented. He offers only his opinion that the *Sodomsky* finding of an

abandoned expectation of privacy was based, in part, on the defendant's failure to ask the right questions at the computer repair shop. In Appellant's view, "the vast majority of people in our society do not understand computers enough to ask the right questions." Brief for Appellant, at 14. He maintains that other jurisdictions have decided cases in a manner consistent with his position. *See U.S. v. Barth*, 26 F.Supp.2d 929 (W.D. TX. 1998) (suppressing evidence found on computer given to a technician for repair on grounds that the defendant retained his expectation of privacy where he gave his computer for the limited purpose of repairing a problem unrelated to the contraband files recovered and where the police search of the computer exceeded the scope of the search conducted by the technician); *State v. Cardwell*, 778 S.E.2d 483 (S.C. Ct. of App. 2015) (disagreeing with the proposition that one has no concept of privacy in a computer and data contained therein when one voluntarily gave the computer to a technician for repair).

Further, while acknowledging that the case is not dispositive, Appellant cites the United States Supreme Court's decision in *Riley v. California*, 134 S.Ct. 2473 (2014), which held that when police lawfully seize a cell phone in a search incident to arrest, they must obtain a search warrant prior to accessing the contents of the cell phone because cell phones contain an abundance of private information and, accordingly, deserve more stringent privacy safeguards. Appellant suggests that because a laptop may contain even more private material than a cell phone, this Court should follow the trend in the law to respect a citizen's privacy in personal data in the computer age.

In response, the Commonwealth first takes the broad position that citizens relinquish their expectation of privacy in closed computer files once they take the computer to a commercial establishment for repair. Based on the theory of abandonment espoused in *Sodomsky*, it submits that when one takes a computer to a commercial repair shop, the individual voluntarily relinquishes control over the computer's contents to the

technician who is a member of the public. Regardless of what type of repairs are necessary, the Commonwealth asserts, the individual has complete control over what he exposes as he can delete private files prior to the repair or limit the technician's access to folders or files on the computer. When the individual does not choose to protect his privacy interest and instead simply hands over his computer to a commercial establishment, the Commonwealth asserts that there is an abandonment of any reasonable expectation of privacy.

The Commonwealth refutes Appellant's argument that private files on a laptop are analogous to financial records disclosed to a bank. Unlike in *DeJohn*, where this Court held that the relinquishment of bank records was not voluntary because one needs a bank account to function in today's society, the Commonwealth reiterates that one retains control over what one exposes to a computer repair shop. *See* Brief for Appellee, at 10 (citing *Sodomsky*, 939 A.2d at 369 (holding that "[c]ontrary to the circumstances in *DeJohn*, *supra*, where a person has little choice but to retain bank accounts in order to function in society, Appellee was not compelled to take this particular computer containing child pornography to the store in the first instance, nor was he forced to leave it there after being informed that the burner's operability would be checked")).

The Commonwealth further distinguishes the High Court's decision in *Riley*, *supra*, which held that police cannot search the contents of a cell phone incident to an arrest without a warrant. It argues that *Riley* has no application to the instant appeal, which is not focused upon the immense amount of information a computer can store but, rather, on the abandonment of a reasonable expectation of privacy by knowingly exposing personal data to the public.

In the event this Court rejects its broad proposition that one abandons his expectation of privacy each time he takes a computer for repair, the Commonwealth

alternatively argues that Appellant abandoned his expectation of privacy under the particular facts presented. It contends that Appellant knew that CompuGig technicians would access his files as he disclosed his computer password to the commercial establishment, authorized it to run diagnostics, was informed that CompuGig needed to do an "OS rebuild with data," and consented to the replacement of his hard drive. The Commonwealth points out that Appellant was not obligated to have the repairs completed, and was free to leave or retrieve his computer at any time. It asserts that there is no evidence that Appellant attempted to keep the files at issue private, considering that he did not remove the contraband files from his computer, did not indicate that there was valuable or private data on the computer, and did not restrict CompuGig's access to the computer in any way.

Thus, the Commonwealth asserts, the record demonstrates that Appellant knowingly and voluntarily granted CompuGig access to his computer files, thereby exposing them to the public and extinguishing his reasonable expectation of privacy. The Commonwealth maintains that other jurisdictions have reached similar results. Brief for Appellee, at 19-21 (citing *State v. Horton*, 962 So. 2d 469 (La. App. 2d Cir. 2007) (holding that the defendant relinquished his reasonable expectation of privacy when he brought his computer to a commercial establishment to have a hard drive installed and his illicit images of child pornography were in a default file, which automatically opened and displayed the unlawful photos to the computer technician); *Rogers v. State*, 113 S.W.3d. 452 (Tex. App. San Antonio 2003) (holding that although the defendant had a privacy interest in his computer hard drive, he did not have complete dominion or control over the files because he had voluntarily relinquished control to the computer repair store and did not take normal precautions to protect his privacy when he expressly directed the computer repair technician to back up the jpeg files)).

Finally, the Commonwealth discusses the private search doctrine. *See* Brief for Appellee at 17 (citing *United States v. Jacobsen*, 466 U.S. 109 (1984), for the proposition that under the private search doctrine, if an individual conducts a search of another's belongings, the police may replicate that search because the reasonable expectation of privacy has been extinguished with respect to that object or container). Acknowledging that police are limited by, and may not exceed, the scope of the private search, the Commonwealth contends that the record here is clear that the police did not exceed the private search. It submits that when Eidenmiller opened the folder containing the illicit photos, they were displayed as larger thumbnails and when Officer Maloney asked to see the images found, he viewed the identical thumbnails that the private search had already revealed.

The Commonwealth finds the Sixth Circuit Court of Appeals' decision in *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015), instructive as it addresses application of the private search doctrine in a case involving the search of digital information. In *Lichtenberger*, the defendant's girlfriend hacked into his computer using a password recovery program, discovered a folder containing child pornography, and informed police of her discovery. The Sixth Circuit Court of Appeals held that there was no Fourth Amendment violation when police viewed the images that the private searcher had viewed because the reasonable expectation of privacy was already frustrated with respect to those images. However, the court held that a subsequent search by police was unlawful because the police exceeded the scope of the prior private search, thereby violating the Fourth Amendment. The Commonwealth reiterates that because the police in no way exceeded the scope of Eidenmiller's private search here, there is no Fourth Amendment violation. According to the Commonwealth, no federal circuit court has found that the private search doctrine is inapplicable to digital containers. Brief of Appellee, at

19 (citing *U.S. v. Tosti*, 733 F.3d 816 (9th Cir. 2013); *Rann v. Atchison*, 689 F.3d 832 (7th Cir. 2012); and *U.S. v. Runyan*, 275 F.3d 449 (5th Cir. 2001)).

In his reply brief, Appellant asserts that the Commonwealth relies upon the private search doctrine in its brief to this Court for the first time in this litigation. He contends that the Commonwealth cites no Pennsylvania case law in support of this doctrine because there is none. Appellant urges this Court not to adopt the private search doctrine as a part of Pennsylvania jurisprudence because there is no record made in the instant case regarding the extent of the private search as compared to the scope of the subsequent police search. Finally, he maintains that the private search doctrine offers the Commonwealth no relief from the warrantless seizure of Appellant's laptop.

III. Analysis

A. Standard/Scope of Review

An appellate court's standard of reviewing the denial of a suppression motion is limited to determining whether the suppression court's factual findings are supported by the record and whether the legal conclusions drawn from those facts are correct. *Commonwealth v. Yandamuri*, 159 A.3d 503, 516 (Pa. 2017). Thus, our review of questions of law is *de novo*. *Id.* Our scope of review is to consider only the evidence of the Commonwealth and so much of the evidence for the defense as remains uncontradicted when read in the context of the suppression record as a whole. *Id.*

B. Private Search Doctrine

We examine first the Commonwealth's assertion regarding applicability of the private search doctrine because if we determine that the doctrine applies, that conclusion would be dispositive of the appeal.[11] The doctrine is illustrated in the United States

[11] Any determination of whether Appellant retained a reasonable expectation of privacy in his laptop when he consented to the replacement of his hard drive presumes that it was the government who invaded his privacy by conducting the search. As explained *infra*,

Supreme Court's seminal decision in *United States v. Jacobson*, *supra*. There, employees of a private freight carrier opened a cardboard package that had been damaged by a forklift and found a closed ten-inch tube wrapped in newspaper. Consistent with company policy regarding insurance claims, the employees cut open the tube to examine its contents and found several plastic bags containing a white powder. By the time a Drug Enforcement Administration ("DEA") agent was summoned, the employees had returned the plastic bags to the tube and replaced the tube in the box. Upon arrival, the DEA agent removed the tube from the box, removed the plastic bags from the tube, field tested the powder to determine if it was cocaine, and concluded that it was. Additional agents subsequently arrived, conducted a second field test, and obtained a warrant to search the mailing address listed on the package.

After being indicted on drug charges, the defendants filed a motion to suppress the evidence recovered from the package, contending that the warrant was the product of an illegal search and seizure. The district court denied suppression. The Court of Appeals reversed, holding that a warrant was required because the testing of the powder constituted a significant expansion of the earlier private search.

The High Court reversed, holding that "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as a result of private conduct." *Jacobsen*, 466 U.S. at 126. The Court explained that "[t]o the extent that a protected possessory interest was infringed, the infringement was *de minimis* and constitutionally reasonable." *Id.* Acknowledging that the Fourth Amendment protects against both unreasonable searches and seizures, the Court defined a "search" as occurring "when an expectation of privacy that society is prepared to consider reasonable

---

once it is determined that the search was conducted absent state action, the inquiry becomes whether the police exceeded the scope of the private search.

is infringed." *Id.* at 113. It defined a "seizure" of property as occurring "when there is some meaningful interference with an individual's possessory interests in that property." *Id.* The Court proceeded to explain that this constitutional protection proscribed only governmental action and was wholly inapplicable "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 government official." *Id.* (citation omitted).

Categorizing the package as an "effect" in which an individual has a reasonable expectation of privacy, the Court observed that a warrantless search of the package would be presumptively unreasonable. *Id.* at 114. However, the Court opined, "the fact that agents of the private carrier independently opened the package and made an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable." *Id.* at 114-15. Accordingly, because the initial invasion of the package was accomplished by private action, the Court held that the Fourth Amendment was not violated, regardless of whether the private action was accidental, deliberate, reasonable, or unreasonable. *Id.* at 115.

Significantly, the High Court explained that the additional invasions of privacy by the government agent "must be tested by the degree to which they exceeded the scope of the private search." *Id.* (citing *Walter v. United States*, 447 U.S. 649 (1980)). The Court observed that "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Id.* at 117. The High Court construed the governmental actions as twofold, first removing the contraband from its packaging and viewing it, and, second, conducting a chemical test of the powder. *Id.* at 118.

Regarding the government agent's reopening of the package after having been told by the employees that it contained a white powder, the Court emphasized that "there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." *Id.* at 119. As the government could use the employees' testimony regarding the contents of the package, the Court found that "it hardly infringed [the defendants'] privacy for the agents to re-examine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube." *Id.* The Court observed that this governmental action did not further infringe upon the defendants' privacy, but rather merely avoided the risk of a flaw in the employees' recollection. *Id.* The High Court held that the defendants "could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents." *Id.* It concluded that the DEA agent's observation of what a private party had voluntarily made available for his inspection did not violate the Fourth Amendment. *Id.*

In the same vein, the Court ruled that the removal of the plastic bags from the tube and the visual inspection of the contents provided the agent with no more information than what had been discovered during the private search. Thus, the High Court opined, the agent's actions "infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment." *Id.* at 120. Notably, the Court explained that while the agent's assertion of dominion and control over the package and its contents constituted a "seizure," the seizure was not unreasonable because the privacy interest in the package had already been compromised, as it had been opened and remained unsealed and because the agent had been specifically invited to examine

the package's contents. *Id.* at 120-21. The Court ruled that "since it was apparent that the tube and plastic bags contained contraband and little else, this warrantless seizure was reasonable, for it is well settled that it is constitutionally reasonable for law enforcement officials to seize 'effects' that cannot support a justifiable expectation of privacy without a warrant, based on probable cause to believe they contain contraband." *Id.* at 121-22.

The High Court proceeded to examine whether the agent's additional intrusion, occasioned by the field test of the white powder, exceeded the scope of the private search. The Court answered this inquiry in the negative, finding that the chemical test that merely disclosed whether a substance is cocaine did not compromise any legitimate interest in privacy as one cannot legitimately have a privacy interest in cocaine, an illegal substance. *Id.* at 123. The Court concluded that because only a trace amount of the material was involved and because the property had been lawfully detained, "the 'seizure' could, at most, have only a *de minimis* impact on any protected property interest." *Id.* at 125. Because the safeguards of a warrant would only minimally advance Fourth Amendment interests, the court concluded that the warrantless "seizure" was reasonable. *Id.*

Contrary to Appellant's assertion in his reply brief, there is ample support for the private search doctrine in Pennsylvania jurisprudence. This Court in *Commonwealth v. Harris*, 817 A.2d 1033, 1047 (Pa. 2002), acknowledged that "[t]he proscriptions of the Fourth Amendment and Article I, § 8, do not apply to searches and seizures conducted by private individuals." We explained that the admission of incriminating letters that had been taken by a private individual and turned over to police did not implicate the Fourth Amendment or Article I, Section 8, because those provisions concern only governmental searches and seizures. *Id.* at 1046. In addition to citing the federal authority discussed

supra, we relied upon this Court's previous decision in *Commonwealth v. Corley,* 491 A.2d 829 (Pa. 1985), which held that the exclusionary rule did not apply to a citizen's arrest because there was no state action. We explained that "[a]t the core of the reasoning underlying this refusal to extend application of the exclusionary rule to private searches is the concept of 'state action,' the understanding that the Fourth Amendment operates only in the context of the relationship between the citizen and the state." *Harris*, 817 A.2d at 1047 (quoting *Corley*, 491 A.2d at 831).

In any event, while Appellant has claimed throughout this litigation that the unlawful search and seizure of his laptop violated both the Fourth Amendment and Article I, Section 8, he has not presented any claim that Article I, Section 8 provides greater protection to abandoned property or that our state counterpart to the Fourth Amendment should extend constitutional privacy protections to private searches under the circumstances here present. Thus, we analyze the case under Fourth Amendment jurisprudence.

C. Application of Private Search Doctrine

Initially, we readily acknowledge that the Commonwealth did not assert the private search doctrine during the suppression hearing and that the parties' arguments instead focused upon whether Appellant had a reasonable expectation of privacy in his laptop when he took the computer to CompuGig for repairs and consented to the replacement of his hard drive. However, we should not ignore governing Fourth Amendment jurisprudence by treating a private search, which is not entitled to constitutional protection, as though it were conducted by a government agent. Moreover, throughout this litigation, the Commonwealth was the nonmoving party or appellee and had no obligation to preserve the issue of whether the private search doctrine applied. *See Rufo v. Bd. of License & Inspection Review*, 192 A.3d 1113, 1123 (Pa. 2018) (observing that appellees

have no obligation to preserve issues). As demonstrated *infra*, we further disagree with Appellant that the record is inconclusive as to whether the requisites of the doctrine are satisfied.

Pursuant to *Jacobson*, our inquiry is two-fold: (1) whether the facts presented establish that a private search was conducted; and, if so, (2) whether the police actions exceeded the scope of the private search. *Jacobsen,* 466 U.S. at 115. Regarding the private nature of the search, we reiterate that Appellant took his laptop to CompuGig for repairs, disclosed his password, and authorized the replacement of his hard drive. While transferring files from the old hard drive to the new one, Eidenmiller discovered the thumbnail images of child pornography. Appellant does not contend that Eidenmiller was in any way acting in concert with law enforcement when this occurred. In fact, Eidenmiller expressly testified at the suppression hearing that he had not been searching for illicit information and had never been asked by law enforcement to keep watch for evidence of child pornography. N.T., 7/7/2016, at 7, 13.

After discovering the contraband images, Eidenmiller then reported the child pornography to his supervisor, and a CompuGig administrative employee contacted the police. *Id.* at 7. In response, Officer Maloney proceeded to the CompuGig facility. The store owners then reiterated that Eidenmiller had found explicit images of young girls on Appellant's laptop and led Officer Maloney back to the computer repair room where Eidenmiller was located. *Id.* at 28. Officer Maloney then asked Eidenmiller to show him what he had found. The relevant testimony in this regard provides:

PROSECUTOR:	What happened when you got to where the computer was?
OFFICER MALONEY:	I spoke with the technician that found the items on the computer.
PROSECUTOR:	Mr. Eidenmiller?

OFFICER MALONEY: Yes, Ma'am.

PROSECUTOR: And what was that conversation?

OFFICER MALONEY: I asked him what kind of images that he saw, what was on the computer, and I also asked him if he could show me what the images were.

PROSECUTOR: Did he do so?

OFFICER MALONEY: Yes.

PROSECUTOR: Did you view those images?

OFFICER MALONEY: I did, yes.

PROSECUTOR: And what were the images that you viewed?

OFFICER MALONEY: The images that I saw were of young females under the age of eighteen, some of them were under the age of I would say thirteen and sexually explicit positions.

PROSECUTOR: And once you viewed those what did you do?

OFFICER MALONEY: I had them shut down the file, and I asked him if there was anything else that needed to be done or anything else that he has and I seized everything.

N.T., 7/7/2016, at 29.[12]

On cross-examination, defense counsel asked Officer Maloney whether Eidenmiller had to "do some clicking around to access the file." *Id.* at 30. Officer Maloney responded in the affirmative. *Id.* Defense counsel then inquired as to whether Eidenmiller opened the file at Officer Maloney's request. *Id.* Officer Maloney replied, "Yes, sir, he showed me the exact route taken to find the images." *Id.*

[12] Officer Maloney explained that he seized Appellant's laptop, an external hard drive containing a copy of Appellant's hard drive, and the power cord. *Id.* at 31. Eidenmiller corroborated Officer Maloney's testimony regarding the conversation that occurred between the two men. *See id.* at 26 (responding in the affirmative when asked whether Officer Maloney asked Eidenmiller to display what he had found).

It has been Appellant's contention throughout these proceedings that when Officer Maloney requested to see the images that Eidenmiller had found while trying to repair Appellant's laptop, an illegal governmental search ensued in violation of his constitutional rights to privacy. Consistent with the High Court's decision in *Jacobsen*, we find this position unpersuasive as it ignores the context of Officer Maloney's request and the fact that CompuGig invited the officer into the establishment to view the very contraband that Officer Maloney asked Eidenmiller to disclose. *See Jacobsen*, 466 U.S. at 119 (explaining that because the government could use the employees' testimony regarding the contents of the package, it "hardly infringed upon [the defendants'] privacy for the agents to re-examine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube;" thus, this governmental action did not further infringe upon the defendants' privacy, but rather merely avoided the risk of a flaw in the employees' recollection). The *Jacobsen* Court explained that the defendants "could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents." *Id.* at 119.

Like the High Court in *Jacobsen*, we conclude that Officer Maloney's observation of what Eidenmiller voluntarily made known to him for his inspection after Officer Maloney was invited to the premises for the express purpose of viewing the contraband did not violate the Fourth Amendment because the private actor's viewing of the images extinguished Appellant's reasonable expectation of privacy in the images of child pornography. Thus, the subsequent police viewing of the contraband was not a "search" under the Fourth Amendment. *See Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971) (providing that when a private actor of her own accord produced evidence such

as guns and clothes for police inspection, "it was not incumbent on the police to stop her or avert their eyes"); *Corely*, 491 A.2d at 832 (holding that the acts of an individual do not "become imbued with the character of 'state action' merely because they are in turn relied upon and used by the state in furtherance of state objectives"). In other words, by the time Officer Maloney viewed the illegal images, Appellant's expectation of privacy in them had already been compromised by Eidenmiller's examinations of the otherwise private information stored in Appellant's computer files.

We next examine whether Officer Maloney's viewing of the images exceeded the search conducted by Eidenmiller. This inquiry is easily determined by the same passage of the suppression hearing testimony cited above. Officer Maloney testified that Eidenmiller showed him "the exact route taken to find the images," *id.,* at 30, and that after viewing the images, Officer Maloney directed Eidenmiller to shut down the computer. *Id.* at 29. The record supports the suppression court's finding that Officer Maloney never expanded upon Eidenmiller's actions, but merely viewed the images that Eidenmiller presented to him. Trial Court Opinion, 10/3/2016, at 11.

Accordingly, Officer Maloney did not exceed the scope of Eidenmiller's private search. As in *Jacobsen*, Officer Maloney's actions infringed upon no legitimate expectation of privacy and, hence, were not a "search" within the meaning of the Fourth Amendment. Also as in *Jacobsen*, Officer Maloney's assertion of dominion and control over Appellant's laptop, which contained the contraband images, constituted a "seizure," although it was not an unreasonable one as the privacy interest in the contraband images, the only information from the laptop revealed to the officer, had already been compromised by the private search. It should not be ignored that police subsequently obtained a warrant to view the remaining files on Appellant's laptop. *See* N.T., 7/7/2016, at 31 (providing that ten days after seizing Appellant's laptop, the police obtained a search

warrant). As noted, *supra* at note 6, Appellant does not suggest that the police independently reviewed the remaining files on Appellant's laptop computer at a time prior to obtaining the warrant.

While not binding on this Court, we find persuasive the decisions of the federal circuit courts of appeals that have applied the *Jacobson* construct to the private search of a computer in a similar manner. To illustrate, in *United States v. Lichtenberger*, *supra*, the defendant's girlfriend hacked into his computer, discovered thumbnail images of adults engaging in sexual acts with minors, and contacted the police. When an officer arrived at the residence, the girlfriend informed him that she hacked the computer belonging exclusively to the defendant and found child pornography. As occurred in the instant appeal, the officer then asked the girlfriend to show him what she had discovered. Unlike the instant case, however, the girlfriend displayed to the officer not only the images that she had recovered during the private search, but also displayed additional images of child pornography. The officer then directed the girlfriend to shut down the computer and seized it.

The defendant was later indicted on charges of child pornography and moved to suppress all evidence obtained pursuant to the officer's warrantless review of the laptop. The defendant contended that when the officer directed the girlfriend to show him what she had found, the girlfriend had become an agent of the government rendering the search impermissible under the Fourth Amendment. The government countered that the Officer's review of the images was valid under the private search doctrine as set forth in *Jacobson*. The district court granted the defendant's suppression motion.

The Sixth Circuit Court of Appeals affirmed the district court's order granting suppression, but did so based only on the second prong of the *Jacobsen* test, finding that the police exceeded the scope of the private search. As an initial matter, the court

concluded that the private search doctrine applied because the defendant's girlfriend acted solely as a private citizen when she searched the defendant's computer, invited the officer into the residence, and showed the officer what she had found. Pursuant to *Jacobsen*, the Court of Appeals agreed with the district court that the case presented an "after-the-fact confirmation of a private search." *Id.* at 484.

The Court of Appeals in *Lichtenberger* viewed the next inquiry under *Jacobsen* as whether the officer's search remained within the scope of the private search. *Id.* at 485. The court acknowledged how "searches of physical spaces and the items they contain differ in significant ways from searches of complex electronic devices under the Fourth Amendment." *Id.* at 487 (referencing *Riley v. California, supra*). The court reasoned that the magnitude of private information retained in a computer manifested itself in *Jacobsen's* requirement that the officer has to proceed with "virtual certainty" that the inspection of the laptop and its contents would not tell the police anything more than they had already learned from the individual who conducted the private search. *Id.* at 488. Stated differently, when the governmental viewing is limited to the scope of the private search, the magnitude of confidential files and information contained in one's computer is protected from the prying eyes of the government unless and until a warrant is obtained. Absent a warrant, the government may view only those files that were disclosed pursuant to the private search.

The *Lichtenberger* court found that this requirement was not satisfied because the officer admitted that he may have asked the girlfriend to open files that she had not previously opened during her private search. *Id.* Finding a lack of certainty that the officer's review was limited to the photographs discovered during the girlfriend's earlier private search, the Court of Appeals held that there was a real possibility that the officer exceeded that search and could have discovered other information on the defendant's

laptop that was private, such as bank statements or personal communications unrelated to the allegations prompting the search. The court concluded that this discovery was precisely what the *Jacobsen* decision sought to avoid in articulating its beyond-the-scope test. *Id.* at 488-89.

The *Lichtenberger* court asserted that it was not alone in its approach to these modern considerations under the Fourth Amendment, as other circuit courts have placed a similar emphasis on "virtual certainty" in their application of *Jacobsen* to searches of contemporary electronic devices. *Id.* at 489-91 (citing *United States v. Runyan*, *supra* (holding that, under *Jacobsen*, police did not exceed the private search of defendant's computer disks where his ex-wife had privately searched them and found child pornography, but did exceed the scope of the private search when police examined disks not viewed during that private search as police had no "substantial certainty" regarding their contents); *Rann v. Atchison*, *supra* (applying *Jacobsen* to a subsequent police viewing of privately searched digital storage devices such as a memory card and computer zip drive that the victim of child pornography and her mother provided to police, and holding that police did not exceed the private search as they were "substantially certain" that the devices contained child pornography based upon the statements of the private parties); *United States v. Tosti*, *supra* (upholding an officer's viewing of contraband under *Jacobsen* where the computer technician repairing the defendant's computer disclosed to police thumbnail images containing child pornography and the police viewed only the images that the technician had already viewed)).[13]

[13] Additional federal circuit court decisions have applied the *Jacobsen* private search construct to searches of digital information stored on electronic devices. *See e.g. United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018) (applying *Jacobsen* to an officer's viewing of the defendant's computer files and concluding that because the child pornography files were deemed suspicious by a private actor and police did not expand the private actor's search, the Fourth Amendment was not violated); *United States v. Johnson*, 806 F.3d

D. Conclusion

In the instant case, we have applied the High Court's accepted *Jacobsen* criteria and have concluded, based on the clear record, that Eidenmiller was not acting as an agent of the government when he discovered the thumbnail images of child pornography, and that Officer Maloney viewed only those images that Eidenmiller had presented to him based on Eidenmiller's private search. As Officer Maloney did not exceed the private search conducted by Eidenmiller, there is no violation of the Fourth Amendment under *Jacobsen*.

We clarify that we are not adopting the Commonwealth's position that one abandons his expectation of privacy in his computer files when he delivers his computer to a commercial retail establishment for repair. Further, we reject as inapplicable the narrower holding of the Superior Court in *Sodomsky* that one abandons his expectation of privacy when he consents to having the computer repaired in a manner that may result in the exposure of private information stored on the computer files. Instead, we hold that

---

1323 (11th Cir. 2015) (applying *Jacobsen* to the private search of a cell phone and concluding that the police exceeded the scope of the private search when the officer viewed a video that the private actor had not viewed); *United States v. Goodale*, 738 F.3d 917 (8th Cir. 2013) (holding that it is immaterial to application of the private search doctrine under *Jacobsen* whether the private party who conducted the search of the defendant's computer had the defendant's consent to turn over to police illegal images discovered on the defendant's computer; so long as the police officer did not exceed the scope of the private search, the Fourth Amendment was not violated); *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012) (holding that the Fourth Amendment was not violated when Yahoo!, Inc. searched an account after receiving an anonymous tip that it contained images of child pornography because there was no evidence that the government had any role in investigating or participating in the private search); *Commonwealth v. Jarrett*, 338 F.3d 339 (4th Cir. 2003) (holding that the search of the defendant's computer conducted by a hacker did not implicate the Fourth Amendment because the hacker was not acting as an agent of the government when he conducted the search).

an individual's expectation of privacy at the moment he relinquishes his computer to a commercial establishment for repair is irrelevant to our constitutional analysis because the computer technicians examining the contents of the computer are private actors, not subject to the restrictions of the Fourth Amendment.[14] Thus, our decision to affirm the lower court's judgment based upon the private search doctrine is not premised upon a preference to avoid the issue presented but, rather, arises from the inapplicability of Fourth Amendment jurisprudence to non-state actors.

We observe that the ramifications of applying an abandonment theory to the facts presented are profound, as the abandonment theory, unlike the private search doctrine, lacks the constitutional safeguard of a restricted scope of the government's subsequent examination of the evidence discovered. Under an abandonment theory, the individual "checks his privacy interest at the door" when he requests a repair that may reveal the contents of private files stored on his computer. Once that expectation of privacy has been abandoned, there is no constitutional protection to be afforded, and the officer who responds to a report of child pornography found on a computer could potentially search every file on it without restriction. Applied to the facts presented, a true application of an abandonment theory would provide that when Officer Maloney arrived at CompuGig to view the images of child pornography found by Eidenmiller, he could have examined all of the files contained on Appellant's laptop, as any expectation of privacy in those files had been abandoned.[15]

---

[14] For this same reason, the federal cases of *United States v. Jones*, 565 U.S. 400 (2012), and *Carpenter v. United States*, 138 S.Ct. 2206 (2018), are inapplicable as they involve government searches and not searches conducted by a private individual.

[15] Additionally, under an abandonment theory the court would examine whether a reasonable person should have known that his private computer files would be revealed during the completion of a particular computer repair. As Appellant cogently argues

Under the private search doctrine, however, as explained *supra*, the officer responding to a report of child pornography found on a computer would be limited to viewing only those images revealed in the private search. Accordingly, application of the private search doctrine to the facts presented more narrowly tailors the scope of the governmental examination of the information revealed by the private search and offers greater protection of the privacy interests involved.

That is not to say that the application of the private search doctrine always affords greater protection. Where an unscrupulous computer technician takes it upon himself to peruse one's personal information contained in various files stored on the computer, unrelated to the requested repair, and that technician later finds and reports to law enforcement images of child pornography, the Fourth Amendment is not implicated so long as the police officer does not exceed the scope of the private search conducted. This unsavory result, however, is not the fault of the application of a flawed legal theory, but rather a consequence of the Fourth Amendment's guarantee against unreasonable searches *by the government*. For these reasons, we conclude that the abandonment rationale employed in *Sodomsky* has no application to searches conducted by private individuals.

Accordingly, we affirm the judgment of the Superior Court on these independent grounds.

Justices Todd, Dougherty and Mundy join the opinion.

Chief Justice Saylor files a dissenting opinion in which Justice Donohue joins.

Justice Wecht files a concurring and dissenting opinion.

herein, the disparity of knowledge of computer operability possessed by average citizens would render this determination difficult to resolve in many cases.

[J-107-2018] [MO: Baer, J.]
IN THE SUPREME COURT OF PENNSYLVANIA
WESTERN DISTRICT

COMMONWEALTH OF PENNSYLVANIA,	:	No. 16 WAP 2018
	:	
Appellee	:	Appeal from the Order of the Superior
	:	Court entered December 21, 2017 at
	:	No. 435 WDA 2017, affirming the
v.	:	Judgment of Sentence of the Court of
	:	Common Pleas of Butler County
	:	entered March 9, 2017, at No. CP-10-
JON ERIC SHAFFER,	:	CR-0000896-2016.
	:	
Appellant	:	ARGUED: December 6, 2018

CONCURRING AND DISSENTING OPINION

JUSTICE WECHT **DECIDED: JUNE 18, 2019**

I concur only in the result that today's learned Majority reaches. The Majority chooses to invoke our discretionary authority to affirm an order upon any basis, and does so on the basis of the "private search" doctrine.[1] I would address instead the question of abandonment of privacy, which is the issue upon which this Court granted *allocatur*. As applied to these facts, this abandonment issue happens to resolve here in the Commonwealth's favor. Accordingly, I would affirm the judgment of sentence, and I join the Majority only insofar as it reaches the same result. As my path to that result diverges from the Majority's, I respectfully dissent from the Majority's rationale.

As the Majority aptly summarizes the history of the case,[2] I reiterate here only those facts and events necessary to this discussion. On May 27, 2016, Jon Shaffer filed a motion seeking suppression of the child pornography seized from his personal computer. As the Majority recounts, Shaffer argued that Officer Christopher Maloney

---

[1] Maj. Op. at 1-2 & n.1.

[2] *Id.* at 2-12.

unconstitutionally searched Shaffer's computer without a search warrant when he directed a CompuGig employee to open the files on Shaffer's computer and then proceeded to view those files. Shaffer argued that neither exigent circumstances nor any other exception to the warrant requirement of our Constitutions[3] justified the warrantless intrusion. Shaffer asserted that he had a legitimate expectation of privacy in the contents of his laptop computer, an expectation which, he maintained, he did not relinquish by providing the computer to CompuGig for repairs.

The Commonwealth responded by arguing that Shaffer abandoned any expectation of privacy that he had in the computer. The Commonwealth relied primarily upon the Superior Court's decision in *Commonwealth v. Sodomsky*, 939 A.2d 363 (Pa. Super. 2007), a case that is both factually and legally similar to the instant dispute.

On July 7, 2016, the trial court held a hearing on Shaffer's suppression motion. Following testimony from CompuGig employee John Eidenmiller and Officer Maloney, the inquiry focused primarily upon the applicability of *Sodomsky*. The trial court found that the facts of this case were close enough to those in *Sodomsky* that the court was bound to apply its rationale. However, the trial court disagreed with the Commonwealth's assertion that Shaffer abandoned his expectation of privacy the moment he delivered the computer to CompuGig. Instead, the trial court determined, it was not until Shaffer requested repairs that he abandoned any expectation that the contents of the computer would be kept private. At that point, Shaffer forfeited any right to challenge Officer Maloney's actions. Consequently, the trial court denied Shaffer's suppression motion,

---

[3] In his brief to this Court, Shaffer invokes both the Fourth Amendment to the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution. *See* Brief for Shaffer at 8. Shaffer does not provide an analysis pursuant to *Commonwealth v. Edmunds*, 586 A.2d 887 (Pa. 1991), in an effort to demonstrate that the Pennsylvania Constitution provides greater protections than its federal counterpart.

and, later sitting as the fact-finder, convicted Shaffer of the charges stemming from the images obtained from the computer.

Initially, what is most important is what did not occur during the suppression proceedings. At no point did the Commonwealth assert that Officer Maloney's actions with respect to the computer were constitutional due to an earlier private search. The Commonwealth placed all of its eggs into the *Sodomsky* basket (which addressed only whether a person has an expectation of privacy in these circumstances), and did not invoke the private search doctrine. The trial court ruled upon expectation of privacy grounds; it did not find that the search was a private one.

Shaffer had no reason to anticipate or rebut any argument that Officer Maloney's warrantless inquiry into the files on his computer was permissible as an extension of CompuGig's private search. More importantly, Shaffer had no opportunity to create a record to defend against such an argument. As the Majority explains, the applicability of the private search doctrine hinges principally upon whether the police officer exceeded the bounds of the private action already undertaken.[4] Given no reason to believe that the Commonwealth would one day claim that the search at issue was a private search, Shaffer had no cause specifically to cross-examine either Officer Maloney or CompuGig's Eidenmiller regarding the particular actions performed by each. In a case involving the private search question, such cross-examination would be undertaken in order to ascertain whether Officer Maloney did, in fact, exceed the parameters of Eidenmiller's actions.

The case continued in the same character before the Superior Court, where the focus of the parties and the appellate panel remained upon Shaffer's expectation of

[4] *See* Maj. Op. at 20 (citing *United States v. Jacobsen*, 466 U.S. 109, 115, 117 (1984)).

privacy in the computer or his abandonment thereof. Once more, the Commonwealth did not raise the argument that the private search doctrine applied, and the Superior Court accordingly did not address that doctrine. The Superior Court held only that Shaffer had abandoned his expectation of privacy in the computer.

We granted allocatur to address the following question:

> Does an individual give up his expectation of privacy in the closed private files stored on his computer, merely by taking his computer to a commercial establishment for service or repair, where the service or repair requested does not render the viewing of the citizen[']s closed private files as foreseeable to either the customer or the computer technician?

See Commonwealth v. Shaffer, 188 A.3d 1111 (Pa. 2018) (*per curiam*). Our order did not mention the private search doctrine, nor can one reasonably argue that the doctrine was fairly encompassed within the stated question. Nor did we direct any briefing or argument on the private search doctrine.[5]

The private search doctrine did not make any appearance in this case until it surfaced as the Commonwealth's third line of argument in its brief to this Court.[6] The Majority relies exclusively upon this tardy assertion to uphold Shaffer's judgment of sentence. Under the "affirm-on-any-basis" jurisprudential device–which alternatively is known as the "right-for-any-reason" doctrine—the Majority undeniably has the

---

[5] As the Majority correctly notes, the failure of the Commonwealth at any point to raise the issue does not amount to waiver of its right to raise it before us now. *See* Maj. Op. at 23-24 (citing *Rufo v. Bd. of License & Inspection Review*, 192 A.3d 1113, 1123 (Pa. 2018)). As the appellee at all stages, the Commonwealth had no burden to preserve any particular issue on pain of waiver. However, as I discuss below, the Commonwealth's failure to do so undermines the notion that an issue raised for the first time before this Court is "of record" for purposes of our ability to affirm an order on any basis, and this failure places the other party at a significant disadvantage in his or her ability to argue successfully to this Court.

[6] *See* Brief for the Commonwealth at 17.

discretionary authority to resolve the case in this manner. But there are compelling reasons not to do so.

I. The Right-For-Any-Reason Doctrine

The "right-for-any-reason" doctrine "allows an appellate court to affirm the trial court's decision on any basis that is supported by the record." *In re A.J.R.-H.*, 188 A.3d 1157, 1175-76 (Pa. 2018) (citing *Ario v. Ingram Micro, Inc.*, 965 A.2d 1194, 1200 (Pa. 2009)).

> The rationale behind the "right for any reason" doctrine is that appellate review is of "the judgment or order before the appellate court, rather than any particular reasoning or rationale employed by the lower tribunal." *Ario*, 965 A.2d at 1200 (citing *Hader v. Coplay Cement Mfg. Co.,* 189 A.2d 271, 274-75 (Pa. 1953)). As the United States Supreme Court has explained, "The reason for this rule is obvious. It would be wasteful to send a case back to a lower court to reinstate a decision which it had already made but which the appellate court concluded should properly be based on another ground within the power of the appellate court to formulate." *Sec. & Exch. Comm'n v. Chenery Corp.*, 318 U.S. 80, 88 (1943).

Id. at 1176 (citations modified).

However jurisprudentially economical the use of the doctrine may be, an appellate court is not bound to utilize it any time it can scour the record and find another basis upon which to affirm. The doctrine is, and always has been, discretionary and prudential. *See id.* at 1176 ("This Court has stated that an appellate court *may* apply the right for any reason doctrine . . . .") (emphasis added); *Commonwealth v. Wholaver*, 177 A.3d 136, 145 (Pa. 2018) ("[I]t is well settled that this Court *may* affirm a valid judgment or order for any reason appearing as of record.") (emphasis added); *E. J. McAleer & Co. Inc. v. Iceland Prod., Inc.*, 381 A.2d 441, 443 n.4 (Pa. 1977) ("We *may*, of course, affirm the decision of the trial court if the result is correct on any ground without regard to the grounds which the trial court itself relied upon.") (emphasis added).

The principal restraint upon an appellate court's discretionary prerogative to apply the right-for-any-reason doctrine arises when the record does not contain a sufficient factual basis to support the new grounds for affirmance. As we explained most recently in *In re A.J.R.-H.*, an appellate court may apply the doctrine if "the established facts support a legal conclusion producing the same outcome. It may not be used to affirm a decision when the appellate court must weigh evidence and engage in fact finding or make credibility determinations to reach a legal conclusion." *In re A.J.R.-H.*, 188 A.3d at 1176 (citing *Chenery Corp.*, 318 U.S. at 88; *Bearoff v. Bearoff Bros., Inc.*, 327 A.2d 72, 76 (Pa. 1974)).

Thus, at the forefront of any inquiry into the propriety of the application of the right-for-any-reason doctrine is the question of whether the newly asserted basis for affirmance is "of record," *i.e.*, whether the basis is supported by the existing factual record. In conducting this inquiry, we should not ignore how the record in this case was created. At no point before or during the evidentiary hearing on Shaffer's motion did the Commonwealth raise the private search doctrine. Although the Commonwealth bears no issue-preservation duty as appellee, the arguments that it advanced in service of its initial burden at the suppression hearing played a significant role in the creation of the factual record.

At the heart of any private search doctrine analysis is the question of whether the police officer's subsequent actions exceeded those of the private citizen who conducted the first search.[7] Had Shaffer been put on notice, actual or constructive, that he would have to rebut a private search argument, then or in the future, his counsel could have conducted the hearing differently, as any reasonably competent lawyer would. To defend against any private search claim, Shaffer's counsel no doubt would have cross-examined

---

[7] *See Jacobsen*, 466 U.S. at 115, 117; *see also* Maj. Op. at 20.

Eidenmiller in detail regarding the steps that the latter took until he eventually discovered the pornographic files. Counsel then would have inquired as extensively into Eidenmiller's actions when Officer Maloney directed him to locate and display the files for the second time. Finally, counsel would have engaged in a similarly detailed examination of Officer Maloney. Only then would Shaffer have a factual record sufficient to oppose a claim of a private search and to argue that any discrepancies between the two searches (assuming that there were discrepancies and that the second search exceeded the first) rendered the private search doctrine inapplicable. At the very minimum, Shaffer should have had the opportunity to create a sufficient record.

I do not maintain that notice always is a necessary precondition to application of the right-for-any-reason doctrine. Rather, under circumstances such as those presented here, the manner in which the record is created is both an important factor in an appellate court's consideration of whether to apply the right-for-any-reason doctrine, and a significant factor in the crucial inquiry of whether the newly asserted basis for affirmance is "of record."

The sole inquiry from the outset of this case up to and through our grant of *allocatur* was whether Shaffer had an expectation of privacy in the laptop computer that he dropped off for repairs at CompuGig. That inquiry differs significantly from one assessing the private search doctrine. As a general matter, there are two essential elements that must be present before any search can be challenged constitutionally. The area searched must be an area in which the person challenging the search has a reasonable expectation of privacy, *see Commonwealth v. Hawkins*, 718 A.2d 265, 267 (Pa. 1998), and the search must be performed by a state actor. *Commonwealth v. Price*, 672 A.2d 280, 283 (Pa. 1996). The former element concerns whether the challenger has a privacy right in the area that was searched. The latter addresses the issue of who conducts the search.

These two elements entail different substantive analyses and examinations, both as to law and as to fact. The factual record created to establish one element cannot automatically be substituted as a sufficient factual record for the other. We cannot graft an evidentiary record focused entirely upon Shaffer's expectation of privacy onto the Commonwealth's new invocation of the private search doctrine. These are apples and oranges.

To find a sufficient record basis for application of the private search doctrine, the Majority highlights a brief exchange between the Commonwealth's attorney and Officer Maloney, as well as two limited interactions between Shaffer's counsel and Officer Maloney.[8] These excerpts cannot suffice as an evidentiary record that would enable a proper analysis of the private search doctrine under the facts and circumstances of this case. The Commonwealth was not attempting to establish that Officer Maloney's examination of the computer did not exceed Eidenmiller's initial actions. More importantly, a brief two question/and two answer exchange between Shaffer's counsel and Officer Maloney that touched inadvertently upon matters that sometime later might be deemed pertinent to the private search doctrine is a far cry from the examination that would be necessary to build a record adequate to evaluate the private actor versus state actor dilemma.

A review of one aspect of those exchanges will illustrate my point. When Officer Maloney was on the stand, Shaffer's counsel asked him whether Eidenmiller, at the officer's request, opened the file containing the pornographic images. Officer Maloney responded, "Yes, sir, he showed me the exact route taken to find the images."[9] The Majority construes this statement as conclusive evidence that Eidenmiller did, in fact, take

---

8 *See* Maj. Op. at 24-25.

9 N.T., 7/7/2016, at 30.

the same exact path in front of Officer Maloney, and, therefore, that Officer Maloney did not (and could not) exceed the scope of the private search. The problem is that Shaffer's counsel did not test that statement through cross-examination. He simply let it go. The reason for the free pass is not difficult to discern. Shaffer's counsel had no reason to know that the parallelism between the two searches would be an issue in the case, or that years later that one answer would form the factual basis to deny his client relief on a newly asserted, and entirely different, legal basis. Instead, counsel let Officer Maloney testify effectively to a legal conclusion without exploring the factual basis for that conclusion, through no fault of his own. No one would anticipate that a case would take on such a different character at the last stage of state appellate proceedings. That counsel, by happenstance or coincidence, stumbled upon one or two questions relevant to the new issue upon which this Court now chooses to focus does not mean that the record suffices for purposes of our discretionary application of the right-for-any-reason doctrine.

Moreover, the problem is not only that the issue is not "of record." The problem also is that it is inequitable to employ our discretionary authority to apply the right-for-any-reason doctrine here, inasmuch as the issue was thrust upon Shaffer only at this very late stage in the proceedings. When the Commonwealth raised the private search doctrine for the first time as its third argument in its brief to this Court, Shaffer was forced to respond to a new legal theory for the first time in his reply brief to this Court. Reply briefs, by rule, must be limited to 7000 words, and may not exceed fifteen pages.[10] But the page limit is not the greatest obstacle that Shaffer must overcome. It is not what puts him at a significant disadvantage, not what hinders his ability to defend against the Commonwealth's newly asserted theory. It is the state of the record in this case that

[10] *See* Pa.R.A.P. 2135(a)(1).

precludes Shaffer effectively from defending against the new claim. The record before this Court is one tailored ("teed up," as we say) specifically to the question of whether Shaffer retained an expectation of privacy in his laptop computer when he turned it over for repairs. It is not a record containing any meaningful evidentiary development of the facts necessary for evaluation of the private search doctrine in the context of this case. Shaffer is forced—in a reply brief—to try to make the record that we have suffice for the record that we need. He is forced to cram the proverbial square peg into a round hole.

The right-for-any-reason doctrine is premised primarily upon the desirability of conserving judicial and prosecutorial resources. Laudable as that goal may be, we still must be judicious in our exercise of discretion, and we should not wield that tool when it would impose upon one litigant an inequitable handicap. We should apply the doctrine only when the newly invoked basis for relief truly is of record, and where the applicability of that new basis is sufficiently clear, such that further proceedings on remand would be a waste of time and resources. That is not the case here.

There is another reason that I would not apply the right-for-any-reason doctrine in this case. As I discuss in greater detail in Part III below, Shaffer's judgment of sentence should be affirmed on the merits of the question upon which we actually granted *allocatur*. In other words, there is no reason to find an alternative basis to affirm when the case, as is, necessitates affirmance on the precise question presented.

II. The Private Search Doctrine

Before proceeding to the merits of the abandonment of privacy question presented by this case, I will assume for the moment that it *would* be an equitable exercise of our discretion to apply the right-for-any-reason doctrine; I do so in order to note my disagreement with the Majority's application of the private search doctrine.

The seminal case regarding the private search doctrine is the Supreme Court of the United States' decision in *Jacobsen*. In that case, a supervisor at an airport location of Federal Express noticed that a forklift had damaged a package. *Jacobsen*, 466 U.S. at 111. Together with the office manager, the supervisor opened the damaged package in order to inventory its contents pursuant to a written insurance protocol. Inside the package was a tube assembled from duct tape. The Federal Express employees cut open the tube and found baggies containing what they believed to be cocaine. Immediately, they called the DEA and returned the baggies to the tube. A DEA agent arrived, removed the baggies from the tube, and examined the substance, which tested positive for cocaine. *Id.* at 111-12. Other DEA agents arrived on the scene and, ultimately, obtained a search warrant based in large part upon the search performed by the first agent. *Id.* at 112.

As the Majority recounts, the Supreme Court considered the DEA agent's initial search as a private search because "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct." *Id.* at 126. Because the initial invasion of privacy occurred at the hands of a private individual, and was not performed by a government agent, the subsequent search by the DEA agent was not unreasonable.

This doctrine poses readily identifiable risks to an individual's right of privacy, and entails a considerable potential for abuse. The private search doctrine essentially places the state actor behind private eyes, allowing a law enforcement officer to go wherever a private person before him has gone. To cabin the potential hazard to privacy rights, the Supreme Court limited the subsequent governmental action to the bounds of the actions of the private individual. Any additional actions "must be tested by the degree to which

they exceeded the scope of the private search." *Id.* at 115 (citing *Walter v. United States*, 447 U.S. 649 (1980)).

More significant to the case *sub judice*, and as another limitation on the private search doctrine, the Supreme Court explained that the DEA's subsequent opening of the package did not exceed the parameters of the initial, private search because "there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell [the DEA agent] anything more than he already had been told." *Id.* at 119. It is this statement that distinguishes the circumstances in *Jacobsen* from Officer Maloney's actions in this case.

In *Jacobsen*, the DEA agent opened a package that contained a tube. In the tube were plastic bags containing cocaine. There was nothing else to find or discover. The DEA's re-examination of the package posed no additional threat to Jacobsen's privacy. It was "a virtual certainty" that the second search would reveal nothing but what the Federal Express employees had found and reported.

The same cannot be said for a personal computer. Regardless of the path taken by CompuGig's Eidenmiller to locate the suspicious files as directed by Officer Maloney, there existed a very real potential for exposure of information not yet discovered by the private search. In 2019, one's personal computer contains a wealth of information, both private and public. Even the screen saver, wallpaper, and names of files on the home screen of a computer can expose private information about the individual who owns the computer. Unlike a duct tape tube that has only one area where items can be stored, a personal computer offers virtually limitless areas for exploration. An inadvertent click on a file or tab could uncover to a state actor private information that was not part of the information collected initially by the private actor. Eidenmiller's navigation of a personal computer at the direction of a police officer does not entail the same "virtual certainty," or

near guarantee, that no other private information could fall into the hands of the law enforcement agent in the same way that the tube in *Jacobsen* did. The tube in *Jacobsen* was a limited vessel, eliminating the possibility that the DEA agent would be able to exceed the bounds of the private search. Indeed, if the tube could be said to have an opposite, that opposite would be a personal computer.

Because nothing in the record as established in this case convincingly demonstrates a "virtual certainty" that Officer Maloney's second, warrantless search would not exceed the scope of the initial private search and would not reveal information other than what Eidenmiller already had discovered, I would find the private search doctrine to be inapplicable in this case in the event that the doctrine was properly before us.

That does not mean that I would reverse the lower courts. For the reasons that follow, I would hold that Shaffer ultimately, though not initially, abandoned his expectation of privacy in the computer.

III. Shaffer's Expectation of Privacy in the Personal Computer

We granted allocatur in this case to consider whether the owner of a personal computer abandons his or her expectation of privacy in closed files on that computer the moment he or she drops it off with a computer repair service. This question necessarily implicates the third-party doctrine. When we accepted this appeal, we provided ourselves with an opportunity to reconsider that doctrine in the context of our modern high-tech world, a world in which the interaction between technology and one's personal information has changed significantly from the past.

In *Katz v. United States*, 389 U.S. 347 (1967), the United States Supreme Court stated for the first time that the Fourth Amendment to the United States Constitution "protects people, not places." *Id.* at 351. *Katz* expanded the protections of the Fourth

Amendment to include those places where one enjoys a reasonable expectation of privacy. This landmark decision marked the beginning of our current understanding that a person, place, area, or thing is protected by the Fourth Amendment if the person asserting the protection seeks to preserve the area or place infringed upon as private, and if the expectation of privacy is one that society would deem reasonable. *See Commonwealth v. Shabezz*, 166 A.3d 278, 288 (Pa. 2017).

The third-party doctrine addresses the question of whether a person's expectation of privacy applies when the object as to which the expectation is asserted is placed in the hands of a third person. Had this case been brought even a decade ago, its resolution as a matter of federal constitutional law would have been relatively straightforward. In *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court of the United States firmly established the third-party doctrine, effectively holding that a person retained no expectation of privacy in materials given over to the possession of a third party. In *Miller*, the Court held that Miller's bank records actually were business records of the bank in which Miller could "assert neither ownership nor possession." *Miller*, 425 U.S. at 440. Further, the records, in possession of a third party, could not be deemed exclusively private to Miller as they were "exposed to [bank] employees in the ordinary course of business." *Id.* at 442. Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the [g]overnment." *Id.* at 443.

In *Smith*, the Supreme Court addressed Smith's claim that he held a reasonable expectation of privacy in a pen register that recorded the outgoing numbers dialed from his landline telephone. The Court rejected Smith's claim, opining that it "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." *Smith*, 442 U.S. at 742. The Court noted that, at the time, telephone companies used

dialed numbers for a variety of legitimate business purposes. When a person makes a call, the *Smith* Court reasoned, he or she voluntarily conveyed the dialed number to the phone company, which received the information in the regular course of business. Thus, as in *Miller*, Smith had assumed the risk that, by dialing a number, he subjected himself to the possibility that the telephone company would turn his dialing information over to the government. The Court explained that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44.

Under a reading of only *Miller* and *Smith*, it would appear that Shaffer could claim no legitimate expectation of privacy in his computer once he turned it over to CompuGig. By doing so, he would be deemed by those precedents voluntarily to have exposed the computer's contents to CompuGig's employees, who received the information in the regular course of their business. The argument would follow that Shaffer assumed the risk that a person working at CompuGig could turn any information found on the computer over to the police.

However, the jurisprudential landscape has evolved since the 1970's. A fair review of the United States Supreme Court's recent cases, beginning with *United States v. Jones*, 565 U.S. 400 (2012), reveals that the *Miller*/*Smith* view of the third-party doctrine now is somewhat antiquated, inasmuch as modern technology has caused the High Court to think differently about third-party interactions. In 2012, the Court in *Jones* confronted the question of whether affixing a GPS device to a person's vehicle and tracking his or her movements—without a search warrant—constitutes a search or seizure under the Fourth Amendment. *Id.* at 402. In deciding that doing so was indeed a search, the Court (in an opinion authored by Justice Scalia) emphasized the intrusiveness that the government's actions entailed: "The Government physically occupied private property for the purpose of obtaining information." *Id.* at 404. The Court had "no doubt" that this was

a search for purposes of the Fourth Amendment. *Id.* The installation of the GPS device effectively was a trespass that, for twenty-eight days, permitted the government to know and evaluate all of Jones' vehicular movements.

Justice Scalia's majority opinion drew two concurrences relevant here. First, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, rejected Justice Scalia's trespass-oriented approach to the case. These four Justices would have simply concluded that attachment of the GPS device to Jones' car was a search because it violated Jones' reasonable expectation of privacy through "the long-term monitoring of the movements of the vehicle he drove." *Id.* at 419. Justice Alito opined that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 430.

Justice Sotomayor authored a concurring opinion in which she questioned whether the "Executive, in the absence of any oversight from a coordinate branch, [should have] a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power . . . ." *Id*. at 416. More importantly for present purposes, Justice Sotomayor opined that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* at 417. Specifically with regard to the "digital age," Justice Sotomayor found the third-party doctrine to be "ill suited" because people now "reveal a great deal about themselves to third parties in the course of carrying out mundane tasks." *Id.* "People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their

Internet service providers; and the books, groceries, and medications they purchase to online retailers." *Id.* In Justice Sotomayor's view, a strict application of the third-party doctrine no longer is feasible. This is an idea that would pick up steam a few years later in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

In *Carpenter*, the Supreme Court granted certiorari to determine "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." *Id*. at 2216. At issue were records obtained from communications between a person's cellular telephone and a cellular tower. Through these records, police could track a person's movement or determine whether that person had been in a particular area during a certain time period.

In a majority opinion authored by Chief Justice Roberts, the Court declined to extend *Miller*'s and *Smith*'s strict third-party doctrine to preclude an expectation of privacy in the cellular tower records. The Court held first that, although *Miller* and *Smith* apply to phone numbers and bank records, the doctrine cannot apply automatically to the cellular tower records at issue. The core inquiry still must be whether society would deem reasonable an expectation of privacy in the area or items that were searched or seized. At the time that *Miller* and *Smith* were decided, few would have imagined a society so technologically advanced, or one in which citizens were so attached to electronic devices. Quoting *Riley v. California*, 573 U.S. 373 (2014) (holding that police must get a warrant before searching a cellular telephone seized incident to an arrest), the Court repeated its view that cell phones have become a "feature of human anatomy," which "tracks nearly exactly the movements of its owner." *Carpenter*, 138 S.Ct. at 2218. Modern people "compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id*.

The Court also found it important that cellular towers do not merely log phone numbers. The towers in actuality compile a comprehensive and detailed record of a person's movements. These towers had generated "seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." *Id.* at 2219. The unique nature of the compilation of data by these towers necessarily overcomes the strict parameters of the third-party doctrine. "[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cellular tower records.]" *Id.* at 2217. Thus, the reach of the earlier third-party doctrine cases has been substantially limited in this context.

That the records technically are compiled for commercial purposes cannot negate a person's expectation of privacy. In *Carpenter*, the government seized records encompassing one hundred and twenty-seven days of activity, "an all-encompassing record of the holder's whereabouts." *Id.* As was the case with the GPS tracker in *Jones*, the "time stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). Like the cell phones themselves, the records "hold for many Americans the privacies of life." *Id.* (citation and quotation marks omitted).

Rejecting a rote application of the third-party doctrine, as advocated by the Government and the dissenting Justices, the *Carpenter* Court explained that the doctrine is rooted in a "reduced" expectation of privacy; it does not mean that a person has no expectation of privacy at all. "[T]he fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'" *Id.* at 2219 (quoting *Riley*, 573 U.S. at 392). Neither *Miller* nor *Smith* relied solely upon the fact that the relevant

materials were in the hands of another. Instead, the Court considered "the nature of the particular documents sought" to determine whether there was "a legitimate expectation of privacy concerning their contents." *Id.* at 2219 (citation and quotation marks omitted).

In dissent, Justice Thomas expressed reservations as to the continued viability of the third-party doctrine, as Justice Sotomayor had done in her concurring opinion in *Jones*. In Justice Thomas' view, the Court approached the case incorrectly, inasmuch as the Court should not have contemplated at all whether a search occurred, but instead should have considered whose property was searched. Justice Thomas noted that the Fourth Amendment protects people from unreasonable searches of "their" places, property, and effects. *Id.* at 2235 (Thomas, J., dissenting). Thus, "*each* person has the right to be secure against unreasonable searches . . . in *his own* person, house, papers, and effects." *Id.* (quoting *Minnesota v. Carter*, 525 U.S. 83, 92 (1998) (Scalia, J., concurring) (emphasis in original)). In *Carpenter*, the cellular tower records did not belong to Carpenter. Thus, according to Justice Thomas, he had no viable Fourth Amendment claim. Notably, this approach would eliminate the third-party doctrine altogether. As long as a person owned the property, he or she could claim a Fourth Amendment violation regardless of who was in possession at the time that the search occurred.

It is noteworthy that both Justices Thomas and Sotomayor have opined that the long standing third-party doctrine is no longer sustainable, albeit for different reasons. Nonetheless, what is important presently is that *Carpenter* itself provides the roadmap to resolving the expectation of privacy issue before us today. Foremost, *Carpenter* expressly rejected the notion that a person loses all expectation of privacy in an object immediately upon it landing in the hands of a third party. The Court emphasized that, while one may have a diminished expectation of privacy in that object, he or she does not invariably forfeit his or her expectation of privacy entirely. Examining *Miller* and *Smith*,

the Court noted that what matters most was not that the materials at issue were in the hands of another, but rather "the nature of the particular documents sought" in ascertaining whether there existed a reasonable expectation of privacy in the contents searched or seized. *Carpenter*, 138 S. Ct. at 2219.

In the modern digital age, personal computers and similar devices are quite like the cellular telephones at issue in *Riley* and the tracking of movements in *Jones* and *Carpenter*. Americans use these computing devices to aid in almost every aspect of their daily lives. We use them to get an education, to discuss politics and current events, to find a romantic partner, and to pay our bills. We store personal digital photographs on them, and engage in personal correspondence. We use computers for work, entertainment, and religion. We chronicle our lives with them. We shop with them. We pay our taxes with them. The personal computer, although not always carried everywhere we go like cell phones, has become equally important to the functioning of our daily lives. A search of a computer can provide the government with a complete snap-shot of a person's private life, revealing information related to every aspect of our lives, including those things we seek to keep most private. "An Internet search and browsing history, for example, can be found on an Internet-enabled [personal computer] and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Riley*, 573 U.S. at 395-96.

Personal computers, like modern cellular telephones, "are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life." *Id.* at 403 (citation and quotation marks omitted). For these reasons, personal computers align with cellular phones, GPS devices, and long-term records of a person's movements, such that the third-party doctrine does not automatically extinguish any and all expectation of privacy that a person has in his or her

computer when it is in the hands of another.[11] The protection of the Fourth Amendment simply "does not fall out of the picture entirely." *See Carpenter*, *supra*.[12]

Nonetheless, that Shaffer maintained some expectation of privacy even though he submitted the computer to CompuGig does not mean that Shaffer retained that expectation forever. It is axiomatic that a person who has an expectation of privacy also can abandon that expectation. *Commonwealth v. Dowds*, 761 A.2d 1125, 1131 (Pa. 2000). Abandonment is a question of intent, and "may be inferred from words spoken, acts done, and other objective facts." *Id.* (citing *Commonwealth v. Shoatz*, 366 A.2d 1216, 1220 (Pa. 1976)).

Presently, Shaffer's words and actions demonstrate clearly that he abandoned his expectation of privacy in the computer.[13] In November 2015, Shaffer's laptop stopped

---

[11] The Majority chooses to resolve this case on the basis of the private search doctrine, concluding that "an individual's expectation of privacy at the moment he relinquishes his computer to a commercial establishment for repair is irrelevant to our constitutional analysis because the computer technicians examining the contents of the computer are private actors, not subject to the restrictions of the Fourth Amendment." Maj. Op. at 32. I disagree. If the expectation of privacy was irrelevant, then the Supreme Court of the United States' analyses in *Smith* (bank records) and *Miller* (pen register) would be irrelevant. In those cases, the Supreme Court held that the defendants could not challenge a subsequent search or seizure of the relevant materials because, once those materials were exposed to a third party, the defendants no longer retained an expectation of privacy in them. The Court did not predicate its holding that the seizures were constitutional on the rationale that the subsequent search did not exceed what was exposed to the third-parties. Moreover, if a person does not hold an expectation of privacy in an item being searched, then it does not matter whether the person performing the search is a private or state actor.

[12] My perspective also is congruent with Pennsylvania's Article I, Section 8 third-party doctrine. *See Commonwealth v. DeJohn*, 403 A.2d 1283 (Pa. 1979) (holding that, contrary to *Miller* and *Smith*, under the Pennsylvania Constitution, a person retains a reasonable expectation of privacy in bank records even though a bank employee would have free access to view the contents contained therein).

[13] The Majority characterizes the application of an abandonment theory to the facts of this case as "profound," and observes that such a theory is less protective (in some instances) of privacy rights than is the private search doctrine. Maj. Op. at 32. To be sure,

operating correctly. He believed that his son had downloaded some files on the computer that had affected its functionality. On November 25, 2015, Shaffer took the laptop to CompuGig for service. On the intake form, Shaffer indicated that the computer had been affected by "Spyware/virus" and that it could not "get the Internet." He also indicated that, after his son had downloaded something, the laptop's performance was riddled by "pop ups."

Shaffer provided CompuGig with his password, to allow CompuGig access to the computer, and he requested restorative services. Eidenmiller performed a basic diagnostic test, which revealed that the hard drive was failing. An administrator from CompuGig called Shaffer and told him of the results of this initial test. The administrator also informed Shaffer that the repairs would cost more than the initial estimate of $160. Shaffer told the administrator that, based upon the diagnostics, he wanted to replace the failing hard drive despite the increased cost. Shaffer then authorized further repairs. Shaffer made no efforts to limit CompuGig's access to any file or folder on the laptop.

---

any time that the state obtains and exercises *carte blanche* authority to invade a person's effects, a profound act occurs, regardless of whether that search occurs because the person has given up any right to challenge the search or because the state actor is merely following the actions of a private citizen. It is true as well that the private search doctrine affords an extra layer of constitutional protection beyond that allowed by the traditional third-party doctrine, inasmuch as the latter necessarily entails an absolute abandonment of any and all privacy interests in the property or item provided to the third party, *i.e.*, the person "checks his privacy interest at the door." *Id.* at 32. I depart from the Majority because, as explained hereinabove, I would not apply the traditional third-party doctrine. The Supreme Court of the United States' case law has evolved to the degree that a person no longer categorically checks his privacy interest at the door, at least when the item now in the hands of a third party is a personal computer. Having retained some privacy in that personal computer, the owner may, by limiting access to certain areas of the device, retain some of his or her privacy interest in it. Put differently, with regard to her personal computer and similar devices, a person does not automatically grant access to all of the files stored anywhere on the computer simply by turning it over for service. Of course, as with Shaffer here, the facts of the case may demonstrate that the person intended to grant unfettered access to the entire computer.

Eidenmiller was not a party to that call, but he continued to work on the laptop. Acting on what he believed was Shaffer's request, Eidenmiller attempted to take an image of the hard drive and to place that image into a new hard drive. Although he successfully imaged the old hard drive, he was unable to insert that image onto a new hard drive. A CompuGig employee once more contacted Shaffer and told him of the failed attempt.

Eidenmiller then determined that the only other way to save the files on the defective hard drive was to manually copy the files and transfer them to the new hard drive one-by-one. CompuGig again contacted Shaffer and informed him that this was the last viable option to save the files. Shaffer consented to the work.

On these facts, Shaffer undeniably abandoned whatever expectation of privacy that he retained in the computer. Thus, by the time that Officer Maloney observed the pornographic photographs, Shaffer was unable to claim an expectation of privacy in the electronic folders in which they were stored. Having no such expectation, Shaffer is not entitled to suppression of those images.

* * *

Determination of whether a person has an expectation of privacy in an area searched is no easy task. It requires consideration of a number of factors, some of which are not always readily apparent. Police officers in the field make these decisions every day across Pennsylvania. Occasionally, and no doubt frustratingly, an appellate court will hold that an officer's estimation of a person's expectation of privacy was erroneous, leading to the suppression of evidence and, possibly, the dismissal of charges.

The risk of such an outcome often can be ameliorated by following the letter of our Constitutions and obtaining a search warrant when probable cause exists. It is true that an officer is not required to get a warrant to search an area in which the suspect has no expectation of privacy. However, simply because an officer is not required to get a

warrant does not mean that he or she cannot (or should not) do so. To obtain a warrant is to provide the subsequent search with an added layer of protection from challenge, inasmuch as the search was authorized by a neutral and detached magistrate. Pre-approval of the search by a judicial officer eliminates the officer's need to make the much riskier decision of determining on the spot whether the subject has an expectation of privacy.

In some instances, it will be patent and obvious that the suspect has no expectation of privacy in the area that the officer seeks to search. However, this is not that case. CompuGig had sole possession of Shaffer's computer. An identified witness informed the police that he observed what he believed to be child pornography on the computer. Clearly, probable cause existed to obtain a warrant to search the computer. Instead of searching the computer immediately, the better (and more constitutionally adherent) practice is to secure the computer and proceed to get a warrant, thereby avoiding the risk of erroneously calculating whether Shaffer had an expectation of privacy.

* * *

For the reasons discussed, I concur in the result reached by the Majority. I dissent as to the Majority's legal analysis.

[J-107-2018][M.O. - Baer, J.]
IN THE SUPREME COURT OF PENNSYLVANIA
WESTERN DISTRICT

COMMONWEALTH OF PENNSYLVANIA,	:	No. 16 WAP 2018
	:	
Appellee	:	Appeal from the Order of the Superior
	:	Court entered 12/21/17 at No. 435 WDA
	:	2017, affirming the judgment of
	:	sentence of the Court of Common Pleas
v.	:	of Butler County entered 3/9/17 at No.
	:	CP-10-CR-0000896-2016
JON ERIC SHAFFER,	:	
	:	
Appellant	:	ARGUED: December 6, 2018

DISSENTING OPINION

CHIEF JUSTICE SAYLOR **DECIDED: JUNE 18, 2019**

On the issue of abandonment, I agree with those courts which have held that a person does not abandon a reasonable expectation of privacy merely by turning a computer over to a repairperson to restore its functionality. *See, e.g, United States v. Barth*, 26 F. Supp. 2d 929, 936-37 (1998); *State v. Cardwell*, 778 S.E.2d 483, 488-89 (S.C. Ct. App. 2015), *aff'd as modified*, 824 S.E.2d 451 (S.C. 2019). For my part, in the computer repair scenario, I am reluctant to find wholesale abandonment absent an express admonition to the defendant that closed files may be opened and viewed non-confidentially in the repair process.

Substantively, my thoughts align more closely with the majority's invocation of the private-search doctrine, since the present circumstances "significantly lessened [Appellant's] reasonable expectation of privacy 'by creating a risk of intrusion [by private

parties] which [was] reasonable foreseeable." *Id.* (quoting *United States v. Paige* 136 F.3d 1012, 1017 (5th Cir. 1998)). Nevertheless, I agree with Justice Wecht that the record has not been appropriately developed to allow for consideration of the application of the doctrine in this case. *See* Concurring and Dissenting Opinion at 3-10.

Finally, to the degree that the private search doctrine applies, it would seem to me that it should only justify a viewing, by authorities, of files that already have been opened in the course of the private search. Here, however, police proceeded to *seize* Appellant's laptop from its place of entrustment without a warrant. *See* Majority Opinion, *slip op.* at 4. Other than relying on the concept of abandonment, the Commonwealth fails to identify an applicable exception to the warrant requirement to justify such seizure.[1]

Concluding, as I do, that the case should turn on the abandonment question, and that Appellant did not completely abandon his expectation of privacy in closed computer files stored on his hard disk, I would reverse the order the Superior Court.

Justice Donohue joins this dissenting opinion.

---

[1] As Justice Wecht has amply demonstrated, many of the conceptual difficulties here arise from the shifting focus, at the present stage, from abandonment to the private search doctrine. *See, e.g.* Concurring and Dissenting Opinion at 3 ("Shaffer had no reason to anticipate or rebut any argument that Officer Maloney's warrantless inquiry into the files on his computer was permissible as an extension of CompuGig's private search."). In these circumstances, I respectfully differ with the majority's approach in faulting Appellant for failing to previously anticipate concerns and considerations relevant to the private search doctrine. *See* Majority Opinion, *slip op.* at 5 n.6.

Closer consideration of exceptions to the warrant requirement other than abandonment might be in order, had this case been developed by the Commonwealth so as to bring such exceptions into play in a timely fashion. Again, the Commonwealth does bear a substantial burden relative to warrantless seizures at a suppression hearing. *See, e.g.*, *In re L.J.*, 622 Pa. 126, 146, 79 A.3d 1073, 1085 (2013).