[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.