

COMMONWEALTH OF PENNSYLVANIA

Appellee

v.

JON ERIC SHAFFER

Appellant

IN THE SUPERIOR COURT
OF
PENNSYLVANIA

No. 435 WDA 2017

Appeal from the Judgment of Sentence Entered March 9, 2017
In the Court of Common Pleas of Butler County
Criminal Division at No: CP-10-CR-0000896-2016

BEFORE: BENDER, P.J.E., OLSON, J., and STABILE, J.

OPINION BY STABILE, J.:

FILED DECEMBER 21, 2017

Appellant, Jon Eric Shaffer, appeals from the March 9, 2017 judgment of sentence imposing an aggregate 6 to 12 months of incarceration followed by 156 months of probation for possession of child pornography (18 Pa.C.S.A. § 6312(d)) and criminal use of a communication facility (18 Pa.C.S.A. § 7512). We affirm.

On November 25, 2015, a computer technician was attempting to save files from the failing hard drive in Appellant's laptop computer when he discovered explicit photographic images of young girls. The technician summoned the police, and the police arrested Appellant and charged him with the aforementioned offenses. Appellant filed a pretrial motion to suppress the evidence from the warrantless search and seizure of his laptop computer. The

trial court conducted a hearing on July 7, 2016, and denied the motion on October 3, 2016. On November 10, 2016, the trial court, sitting as finder of fact, found Appellant guilty of both charges. The trial court imposed sentence on March 9, 2016, and Appellant filed this timely appeal on March 14, 2017.

The trial court summarized the pertinent facts:

[Appellant] delivered his laptop computer to CompuGig for repair and completed an initial work order form that is dated November 25, 2015. On the form, in response to the question, 'What problems are you experiencing?', boxes next to 'Spyware/virus' and 'Can't get to Internet' are marked. Additional information provided by [Appellant] at the time he delivered the laptop to CompuGig indicated that 'Customer's son downloaded some things and now there are a lot of pop-ups. Internet has stopped working.' After running initial diagnostics, [computer technician Justin] Eidenmiller believed the computer had a failing hard drive. A telephone call was made to [Appellant] by CompuGig's administration. During that call [Appellant] indicated that he wished to replace the hard drive on the laptop. Mr. Eidenmiller was not privy to the phone call. Mr. Eidenmiller attempted to 'take an image of the hard drive and put it on a new hard drive at the customer's request.' While the hard drive was able to be imaged, the procedure of transferring the image successfully was unable to be completed. Another call was apparently placed to [Appellant] regarding the matter. In an attempt to move data from the failing hard drive to a new drive, Mr. Eidenmiller manually opened various portions of the data contained in the failing hard drive. In doing so, Mr. Eidenmiller observed the evidence which [Appellant] is seeking to suppress. Mr. Eidenmiller fist [sic] attempted to copy the entire folder that contained the evidence at issue without opening it, but was unable to do so. He then opened the folder in order to copy the within files manually. At that point he observed the files at issue in the form of thumbnail images. Mr. Eidenmiller notified his boss of the discovery.

The police were then called and Officer [Christopher] Maloney arrived, he spoke both to the owners of CompuGig and, after being handed the work order and escorted to the tech area by the owners, to Mr. Eidenmiller. Mr. Eidenmiller then went to

where [Appellant's] laptop computer was located on a bench inside the tech area. Mr. Eidenmiller showed Officer Maloney, at the officer's request, the evidence [Appellant] is seeking to suppress. Mr. Eidenmiller prepared a statement for Officer Maloney and Officer Maloney took possession of the computer and hard drive that had been delivered to CompuGig, as well as other equipment. At a later date, warrants to search the laptop and accompanying hardware were secured by Detective Matthew Irvin of the Cranberry Township Police Department.

Trial Court Opinion, 10/3/16, at 2-3 (record citations and footnotes omitted).

The only issue before us is whether the trial court properly suppressed evidence from the initial warrantless search and seizure of his laptop computer. Our standard of review is as follows:

[An appellate court's] standard of review in addressing a challenge to 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. Because the Commonwealth prevailed before the suppression court, we may 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 record as a whole. Where the suppression court's factual findings are supported by the record, [the appellate court is] bound by [those] findings and may reverse only if the court's legal conclusions are erroneous. Where ... the appeal of the determination of the suppression court turns on allegations of legal error, the suppression court's legal conclusions are not binding on an appellate court, whose duty it is to determine if the suppression court properly applied the law to the facts. Thus, the conclusions of law of the courts below are subject to plenary review.

Commonwealth v. Smith, 164 A.3d 1255, 1257 (Pa. Super. 2017). Article 1, Section 8 of the Pennsylvania Constitution precludes warrantless searches of private property. PA. CONST. art. I, § 8. "Absent the application of one of a few clearly delineated exceptions, a warrantless search or seizure is

presumptively unreasonable. *Commonwealth v. Williams*, 73 A.3d 609, 614 (Pa. Super. 2013) (quoting *Commonwealth v. Whitlock*, 69 A.3d 635, 637 (Pa. Super. 2013)), appeal denied, 87 A.3d 320 (Pa. 2014).

Both parties and the trial court rely heavily on *Commonwealth v. Sodomsy*, 939 A.2d 363 (Pa. Super. 2007), another case in which a computer technician discovered child pornography on a customer's computer. The *Sodomsy* Court concluded, under the circumstances there present, that the customer relinquished his privacy expectation in the contents of his hard drive. The Commonwealth and the trial court find *Sodomsy* controlling, while Appellant argues that it is distinguishable and/or that it should be overturned.

In *Sodomsy*, the defendant took his computer to a Circuit City and requested installation of an optical drive and DVD burner into his computer. *Id.* at 364. The store informed the defendant that it would run tests to confirm the DVD burner was working, but did not describe that testing process in detail. *Id.* In order to test the newly installed DVD burner, the technician ran a "general search for a video" to be burned to a disc. *Id.* at 365. The search returned a number of files, some of which "appeared to be pornographic in nature due to their titles which included masculine first names, ages of either thirteen or fourteen, and sexual acts." *Id.* at 365-66. The technician clicked on "'the first one' that appeared questionable, and the video contained the lower torso of an unclothed male, and when a hand approached the male's

penis, [the technician] immediately stopped the video.” *Id.* at 366. The technician summoned police, as he had been told to do by a state police officer under such circumstances. *Id.* Police responded, viewed the video clip the technician had seen, and seized the computer. *Id.* Subsequently, they obtained a warrant and discovered child pornography. *Id.*

The trial court granted the defendant’s motion to suppress. Central to the dispute was whether and to what extent the defendant abandoned his privacy interest in the computer while it was at Circuit City for the requested work. The trial court reasoned that the defendant did not expect his computer’s contents to be published to anyone other than Circuit City employees. *Id.* at 367.

In canvassing the law of abandonment, the Sodomsky Court noted, “[t]he issue is not abandonment in the strict property-right sense, but whether the person prejudiced by the search had voluntarily discarded, left behind, or otherwise relinquished his interest in the property in question so that he could no longer retain a reasonable expectation of privacy with regard to it at the time of the search.” *Id.* at 366-67 (quoting *Commonwealth v. Shoatz*, 366 A.2d 1216, 1220 (Pa. 1976)). Furthermore, “the Fourth Amendment protects people, not places. What 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)).

In light of these principles, the Sodomsky Court determined that the proper inquiry 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.* In other words, did the defendant “give access or knowingly risk access to his video files.” *Id.* at 368. This Court disagreed with the trial court’s analysis because “if [the defendant] exposed the video contents of his computer to Circuit City employees, he abandoned his privacy interest in those computer contents because those employees were members of the public.” *Id.*

Applying these principles, the Sodomsky Court noted that the defendant requested installation of a new DVD drive and was informed that the DVD drive would be tested once installed. *Id.* He did not inquire about the testing process or restrict Circuit City’s access to his files for purposes of running that test. *Id.* Further, Circuit City employees discovered the illicit material while they were testing the DVD drive in a “commercially-accepted manner.” *Id.* The employees were free to choose any video file from the list of videos to run the test. *Id.* at 369. In addition, the Sodomsky Court noted that the defendant’s actions—bringing his computer to Circuit City, requesting

repairs, and failing to remove or rename the illicit files beforehand—were volitional. *Id.* at 369.

The Sodomsy Court distinguished *Commonwealth v. DeJohn*, 403 A.2d 1283 (Pa. 1979), cert. denied, 444 U.S. 1032 (1980), wherein our Supreme Court held that banks cannot disclose their customers' financial records without a search warrant. The DeJohn Court reasoned:

[T]he disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. [...] To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.

Id. at 1289–90.

Similarly, the Sodomsy Court distinguished *Commonwealth v. Davis*, 743 A.2d 946 (Pa. Super. 1999), in which this Court held that tenants retain a privacy interest in rented property despite a landlord's right of access. Thus, police subjected the tenant to an unreasonable search and seizure despite the landlord's consent to enter the property. *Id.* at 951-52.

Ultimately, the Sodomsy Court concluded that the defendant did not retain a privacy interest in his video files under the circumstances of that case. *Sodomsy*, 939 A.2d at 369. "If a person is aware of, or freely grants to a

third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and lost any reasonable expectation of privacy in those contents.” *Id.*

Appellant first argues that that *Sodomskey* should be overruled. Appellant’s Brief at 11-15. That action must come, if at all, from an en banc panel of this Court or from our Supreme Court. See *Commonwealth v. Taggart*, 997 A.2d 1189, 1201 n.16 (Pa. Super. 2010) (noting that one three-judge Superior Court panel cannot overrule another).

Appellant next argues that *Sodomskey* is distinguishable. In essence, Appellant argues that he did not give or knowingly risk access to the illicit photographs in his hard drive because the possibility of their discovery was extremely remote, given his initial reasons for leaving his computer with CompuGig. As noted above, Appellant stated that he could not access the Internet and that he believed his laptop was infected by spyware or a virus. He did not anticipate that his hard drive was failing. Nonetheless, the record indicates that CompuGig contacted Appellant after Eidenmiller discovered the failing hard drive, and Appellant requested that the hard drive be replaced. Given his consent to the hard drive replacement, Appellant’s original description of the problem is irrelevant to our analysis.

Appellant also argues that he did not anticipate—and was never told—that CompuGig might need to access individual files in order to salvage data. He notes that CompuGig first tried to take an image of the entire hard drive

and, when that failed, tried to copy individual folders and, when that failed, opened folders to copy individual files. The illicit photographs happened to be in a folder that would not copy. Appellant argues that this chain of events was unforeseeable, and that he therefore did not legally abandon his privacy interest in the illicit photos within the meaning of *Sodomsky*.

We believe Appellant reads *Sodomsky* too narrowly. There, unbeknownst to the defendant, the technician intended to run a test using a video file from the defendant's hard drive. See *Sodomsky*, 939 A.2d at 364. The defendant did not ask how that would be done, nor did he restrict the means of doing so. See *id.* Thus, the defendant was uninformed and unaware of the possibility that the technician would search video files on the defendant's computer. Similarly, in this case, Appellant was unaware and did not inquire into the details of the procedure he authorized. The record reflects that, on November 30, 2015, five days after Appellant dropped his computer off for service, CompuGig called Appellant and informed him his hard drive was failing. N.T. Hearing, 7/7/16, at Exhibit A. Appellant authorized CompuGig to replace the hard and install an image of the failing drive. *Id.* Four days later, on December 4, 2015, a CompuGig administrator called Appellant to "explain that we must do an OS rebuild with data." *Id.*¹ Appellant

¹ Appellant insists he received only one phone call from CompuGig after his initial visit. Appellant's Brief at 17. Appellant ignores the applicable standard of review, pursuant to which we "consider only the evidence of the

was informed that CompuGig intended to install a new hard drive and transfer data from the old one. *Id.* at 20.

We find this case slightly distinguishable from *Sodomsky* in several respects, but in those respects it favors the trial court's order. The *Sodomsky* defendant was unaware that the technician would need to access any of his files. Here, in contrast, Appellant was informed that CompuGig needed to copy and transfer all his files. In *Sodomsky*, the technician noticed incriminating titles attached to the illicit video files, and he confirmed his suspicions by opening and beginning to play one of the files. Instantly, the illicit images appeared as thumbnail files when Eidenmiller opened a folder on Appellant's hard drive, and they immediately appeared² to Eidenmiller to be sexually explicit depictions of underage children. He conducted no further investigation. We cannot reasonably distinguish *Sodomsky* on grounds that

Commonwealth and so much of the evidence for the defense as remains uncontradicted when read in the context of the record as a whole." *Smith*, 164 A.3d at 1257. The record contradicts Appellant's assertion that he received only one phone call.

² The *Sodomsky* Court expressed no opinion on whether the defendant abandoned his privacy interest in other files, such as e-mail or financial records. *Sodomsky*, 939 A.2d at 369. Similarly, we do not address whether and to what extent a person retains a privacy interest in e-mails, financial records, or other files whose incriminating nature might not be immediately obvious to a technician who accesses them in the ordinary course of performing a requested service.

Eidenmiller's methods were unnecessarily intrusive or unforeseeable, as compared to those employed in *Sodomsky*.

In other respects, the two cases are similar. Appellant, like the *Sodomsky* defendant, did not inquire about or restrict the means of completing the requested service. The *Sodomsky* Court noted the Circuit City technicians were "testing the DVD drive's operability in a commercially accepted manner rather than conducting a search for illicit items." *Sodomsky*, 939 A.2d at 368. Likewise, in this case, Eidenmiller was not searching for illicit photographs. He discovered the photographs during a file-by-file transfer after broader, less intrusive means of transferring the data failed. Nothing in the record suggests that Eidenmiller failed to use a commercially accepted manner of performing the work Appellant requested.

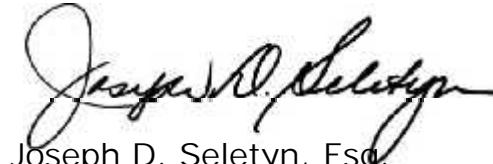
In short, we find *Sodomsky* controlling. As noted above, the *Sodomsky* Court concluded that abandonment occurs when a person "freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents." *Id.* at 370. If the *Sodomsky* defendant granted potential access to his illicit files under the circumstances there present, Appellant clearly did so in the instant case.³

³ Appellant seeks to avoid this result by relying on *United States v. Jones*, 565 U.S. 400 (2012), in which the Supreme Court ruled that, for Fourth Amendment purposes, police engage in a search when they place a GPS unit

For all of the foregoing reasons, we discern no error in the order denying Appellant's motion to suppress evidence. We therefore affirm the judgment of sentence.

Judgment of sentence affirmed.

Judgment Entered.

A handwritten signature in black ink, appearing to read "Joseph D. Seletyn". The signature is fluid and cursive, with a large initial "J" and "S".

Joseph D. Seletyn, Esq.
Prothonotary

Date: 12/21/2017

in a person's vehicle. Relying on Jones, Appellant claims police "physically occupied" and "trespassed upon" Appellant's computer when they retrieved the illicit files without a warrant. Appellant's Brief at 21. We find Jones inapposite, and Appellant's reliance on it is not responsive to the trial court's finding that he abandoned his privacy interest in the illicit files.