2026 PA Super 81

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF PENNSYLVANIA
v.	:	
EDWARD JOSEPH ZEALOR	:	
Appellant	:	No. 825 EDA 2025

Appeal from the Judgment of Sentence Entered February 26, 2025
In the Court of Common Pleas of Montgomery County Criminal Division
at No(s): CP-46-CR-0000986-2024

BEFORE: LAZARUS, P.J., DUBOW, J., and SULLIVAN, J.

OPINION BY SULLIVAN, J.: **FILED APRIL 22, 2026**

Edward Joseph Zealor ("Zealor") appeals from the judgment of sentence following his convictions for fifty counts of possessing child sexual abuse material arising from his possession of thousands of photographs and videos of child pornography.[1] Because Zealor's appellate issues hinge on the trial court's denial of his suppression motion, and none of his issues merit relief, we affirm the judgment of sentence.

The trial court set forth the factual and procedural history of this case, which we set forth in relevant part, as follows:

> [I]n February [] 2024, [the] Pennsylvania State Police ["PSP")] filed a criminal complaint charging Zealor with[, *inter alia*, several counts of disseminating and possessing child pornography.] . . ..
>
> [I]n August [] 2024, Zealor filed a motion to suppress evidence, alleging that the Commonwealth unlawfully obtained information from Comcast Cable through the Commonwealth's

---

[1] ***See*** 18 Pa.C.S.A. § 6312(d).

service of administrative subpoenas directed to Digital Media, LLC and Comcast Cable [pursuant to section 5743.1 of Pennsylvania's Stored Wire and Electronic Communications and Transactional Records Access Act ("the Act")[2]]. Zealor claimed the administrative subpoenas are not constitutionally valid. The administrative subpoenas formed the basis for a search warrant of Zealor's apartment, which Zealor claimed did not contain sufficient probable cause to justify the searches and seizures.

On September 20, 2024, the court held a hearing on Zealor's motion to suppress evidence. Zealor waived his presence at the suppression hearing. At the suppression hearing, no testimony was presented. The Commonwealth entered five exhibits into evidence: (1) [a] stipulation of facts; (2) designation of Deputy Attorney General [("DAG")] Kristen Kemp to issue administrative subpoenas; (3) administrati[ve] subpoena on Comcast; (4) administrative subpoena on Digital Media; and (5) search warrant for 1514 W Marshall Street, Norristown, PA (West Norriton Township, Montgomery County).

At the suppression hearing, the parties stipulated to the following facts. In the [f]all of 2023, Corporal Anthony Reppert [("Corporal Reppert")] of the [PSP] worked as a member of the Internet Crimes Against Children Task Force. As a part of the task force, Corporal Reppert monitors BitTorrent [peer-to-peer ("P2P")] file sharing networks for possible sharing and trading of child pornography . . .. The investigation in this case began when Corporal Reppert received a notification that IP address 173.12.32.109 may be sharing child pornography. [I]n November [] 2023, Corporal Reppert successfully downloaded numerous files that were coming from a computer using th[is same] IP address of 173.12.32.109. Within the files downloaded was a video depicting a [two-to-four-]year-old child being sexually assaulted by an adult male. [I]n December [] 2023, [DAG] Kemp approved an administrative subpoena for the IP address of 173.12.32.109 to be served on Comcast. Comcast responded with subscriber information relating back to a Digital Media, LLC [("Digital Media")] with a subscriber address [for Jefferson Apartments] in Norristown. [I]n January [] 2024, [DAG] Kemp approved another administrative subpoena for [the] IP address of 173.12.32.109 to be served on Digital Media[,] LLC. [I]n January [] 2024, Corporal

---

[2] ***See*** 18 Pa.C.S.A. § 5741 *et seq*.

Reppert received the results from Digital Media[; and Corporal Reppert learned that the IP address was a public facing IP address shared by all internet connections at Jefferson Apartments, with each subscriber possessing a network gateway, such as a router, with a unique port number, through which the subscriber could use the shared IP address to access the internet and make connections with other IP addresses. Corporal Reppert learned from the subpoena that Zealor's port number used the shared IP address to communicate *via* a P2P program with other IP addresses associated with child pornography, and Zealor's combined IP address and port number was associated with a unique torrent identifier—called an "infohash," discussed further ***infra***—for child pornography]. Based on that information, Corporal Reppert applied for a search warrant for [Zealor's] home in West Norriton, Montgomery County, PA. The search warrant was signed and authorized by [Magisterial District Judge] Edward Kropp. The attorneys presented argument. Following the suppression hearing, the court took the motion under advisement.

[I]n October [] 2024, the court issued findings of fact and conclusions of law and denied Zealor's suppression motion. The court scheduled this matter for a bench trial [i]n November [] 2024. [I]n November [] 2024, Zealor signed a waiver of jury trial and a stipulated bench trial colloquy and proceeded with a stipulated bench trial. The Commonwealth filed [a]mended [b]ills of [i]nformation in open court charging Zealor with[, *inter alia*,] fifty [] counts of [possessing child pornography] . . ..

Following the stipulated bench trial, the court found Zealor guilty of [the fifty] counts of [possessing child pornography]. The court determined that Zealor possessed a total of 41,663 photographs and 9,571 videos. The court deferred sentencing to obtain a presentence investigation report, a sexual violent predator assessment and a psychosexual evaluation, and released Zealor on . . . bail.

[I]n February [] 2025, the court held a sentencing hearing. For counts [one] through [forty-nine], the court imposed concurrent sentences of two-and-a-half to seven years in a state correctional institution. That sentence is in the standard range of the guidelines. On [c]ount [fifty], the court imposed seven years of probation consecutive to the expiration of parole.

> On March 25, 2025, Zealor filed a timely [n]otice of [a]ppeal . . ..

Trial Court Opinion, 5/29/25, at 1-4 (some citations to the record omitted).

Both Zealor and the trial court complied with Pa.R.A.P. 1925.

Zealor raises the following issues for our review:

> I. Did the lower court err in denying [Zealor's] motion to suppress[,] pursuant to the 4th Amendment of the United States Constitution and Article I, § 8 of the Pennsylvania Constitution[,] in that the administrative subpoenas issued to Comcast and Digital Media pursuant to [section] 5743.1 allowed the Commonwealth to obtain constitutionally protected information and data without a warrant supported by probable cause and issued by a neutral and detached magistrate or other judicial authority?
>
> II. Did the lower court err in denying [Zealor's] motion to suppress pursuant to the 4th Amendment of the United States Constitution and Article I, § 8 of the Pennsylvania Constitution[,] in that the administrative subpoenas issued to Comcast and Digital Media pursuant to [section] 5743.1 allowed the Commonwealth to obtain constitutionally protected information and data that were beyond the scope of the items listed in [section] 5743.1 without a warrant supported by probable cause and issued by a neutral and detached magistrate or other judicial authority?
>
> III. Did the lower court err in denying [Zealor's] motion to suppress pursuant to the 4th Amendment of the United States Constitution and Article I, § 8 of the Pennsylvania Constitution[,] in that the administrative subpoenas issued to Comcast and Digital Media pursuant to [section] 5743.1 were served on foreign corporations outside the boundaries of Pennsylvania, over which the Commonwealth had no jurisdiction, in violation of the Uniform Act to Secure Attendance of Witnesses from Without the State in Criminal Cases, 42 Pa.C.S.A.] § 5964?

Zealor's Brief at 3 (unnecessary capitalization omitted).

Our standard of review for an order denying a suppression motion is as follows:

> [We are] 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, we are bound by these findings and may reverse only if the court's legal conclusions are erroneous. Where, as here, 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 our plenary review.

Commonwealth v. Ross, 330 A.3d 1262, 1267 (Pa. Super. 2025) (internal citation and quotations omitted).

Because all of Zealor's issues relate to his challenge to the issuance of administrative subpoenas pursuant to section 5743.1, we begin by setting forth the relevant portions of section 5743.1, which provide:

> **(a) Authorization.—**
>
> (1) In an ongoing investigation that monitors or utilizes online services or other means of electronic communication to identify individuals engaged in an offense involving the sexual exploitation or abuse of children, the following shall apply:
>
> (i) The following may issue in writing and cause to be served a subpoena requiring the production and testimony under subparagraph (ii):

* * * *

(B) A deputy attorney general designated in writing by the Attorney General.

* * * *

(ii) A subpoena issued under subparagraph (i) may be issued to a provider of electronic communication service or remote computing service:

(A) requiring disclosure under section 5743(c)(2) (relating to requirements for governmental access) of a subscriber or customer's name, address, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, which may be relevant to an authorized law enforcement inquiry;

* * * *

(2) A subpoena under this section shall describe the information required to be produced and prescribe a return date within a reasonable period of time within which the information can be assembled and made available.

* * * *

(b) Service.--The following shall apply:

* * * *

(3) Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name by delivering the subpoena to any of the following:

(i) An officer of the entity.

(ii) A managing or general agent of the entity.

(iii) An agent authorized by appointment or by law to receive service of process in this Commonwealth.

(4) The affidavit of the person serving the subpoena entered on a true copy of the subpoena by the person serving it shall be proof of service.

(c) Enforcement.--The following shall apply:

(1) The Attorney General or a district attorney, or a designee may invoke the aid of a court of common pleas within the following jurisdictions to compel compliance with the subpoena:

(i) The jurisdiction in which the investigation is being conducted.

(ii) The jurisdiction in which the subpoenaed person resides, conducts business or may be found.

(2) The court may issue an order requiring the subpoenaed person to appear before the Attorney General or a district attorney, or a designee to produce records or to give testimony concerning the production and authentication of the records. A failure to obey the order of the court may be punished by the court as contempt of court. All process may be served in a judicial district of the Commonwealth in which the person may be found.

* * * *

18 Pa.C.S.A. § 5743.1.

In his first issue, Zealor asserts the information the Commonwealth sought in its administrative subpoenas was constitutionally protected and

obtained without a warrant.[3] Initially, we note that under both the Fourth Amendment to the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution, searches conducted without a warrant are *per se* unreasonable unless a recognized exception applies. ***See***, ***e.g.***, ***Hunte***, 337 A.3d at 498. Once a defendant files a motion to suppress, "it is the Commonwealth's burden to prove, by a preponderance of the evidence, that the challenged evidence was not obtained in violation of the defendant's rights." ***Commonwealth v. Wallace***, 42 A.3d 1040, 1047-48 (Pa. 2012). However, "a defendant must show that he had a privacy interest in the place invaded or thing seized that society is prepared to recognize as reasonable." ***Commonwealth v. Enimpah***, 106 A.3d 695, 698-99 (Pa. 2014) (explaining

---

[3] We note Zealor's brief is not a paragon of clarity. His argument at times implies a constitutional challenge to section 5743.1. ***See*** Zealor's Brief at 10-11, 15 (stating that a "statute cannot authorize what the Fourth Amendment or Article I, Section 8 would prohibit," and citing, *inter alia*, ***Commonwealth v. Hunte***, 337 A.3d 483, 497–98 (Pa. 2025) wherein our Supreme Court struck down an implied consent statute following a challenge to the statute as facially unconstitutional). However, section 5743.1 is presumed constitutional, and Zealor does not develop an argument that ***all*** of its applications are unconstitutional. ***See*** Zealor's Brief at 10-15; ***cf***. ***Hunte***, 337 A.3d at 497-98. Additionally, it is unclear whether Zealor is asserting an as-applied constitutional challenge to the statute. ***See generally Commonwealth v. Hairston***, 249 A.3d 1046, 1054 n.5 (Pa. 2021) (stating that an as-applied challenge to a statute's constitutionality "is one asserting that the statute, even though it may generally operate constitutionally, is unconstitutional in a defendant's particular circumstances"). However, to the extent Zealor brings an as-applied challenge, it would hinge on the constitutionality of the information sought by the Commonwealth, and, as such, our analysis ***infra*** addresses the same issue.

the important distinction between standing and privacy interest). A reasonable expectation of privacy will be found to exist when the defendant "exhibits an actual or subjective expectation of privacy and that expectation is one that society is prepared to recognize as reasonable." ***Commonwealth v. Kurtz***, 294 A.3d 509, 520 (Pa. Super. 2023), *aff'd*, 348 A.3d 133 (Pa. 2025).

In determining whether an individual's expectation of privacy is legitimate or reasonable, we must consider the totality of the circumstances and the determination "ultimately rests upon a balancing of the societal interests involved." ***Commonwealth v. Peterson***, 636 A.2d 615, 619 (Pa. 1993). "The constitutional legitimacy of an expectation of privacy is not dependent on the subjective intent of the individual asserting the right but on whether the expectation is reasonable in light of all the surrounding circumstances." ***Commonwealth v. Burton***, 973 A.2d 428, 435 (Pa. Super. 2009) (*en banc*) (citation omitted). "The expectation of privacy is an inquiry into the validity of the search or seizure itself; ***if the defendant has no protected privacy interest, neither the Fourth Amendment nor Article I, § 8 is implicated***." ***Enimpah***, 106 A.3d at 699 (emphasis added).

Relevant to digital information, this Court has recently articulated the law regarding the "third-party doctrine," *i.e.*, when a defendant voluntarily turns over information to third parties, as follows:

> It is well-established that, under the third-party doctrine, an individual may forfeit his or her legitimate privacy interest in

property that is voluntarily provided to others as he has taken the risk that that information would be conveyed by the third party to the government. ***See Commonwealth v. Pacheco***, [] 263 A.3d 626, 636 & n.10 ([Pa.] 2021). In ***United States v. Miller***, 425 U.S. 435 [] (1976), the United States Supreme Court held that a bank customer holds no protected privacy interest under the Fourth Amendment in his account records, including copies of checks and deposit slips. [***See i***]***d***. at 440-43 . . .. Following ***Miller***, our Supreme Court has ruled that Article I, Section 8 of the Pennsylvania Constitution provides broader protection to ***substantive*** bank records than the Fourth Amendment but that a bank customer has no legitimate expectation of privacy over basic account information, such as the name and address associated with an account. [***See***] ***Commonwealth v. Duncan***, [] 817 A.2d 455, 462-63 ([Pa.] 2003); ***Commonwealth v. DeJohn***, [] 403 A.2d 1283, 1290-91 ([Pa.] 1979).

The third-party doctrine has also been extended to computer files, electronic messages, and other digital records. In ***Commonwealth v. Dunkins***, [] 263 A.3d 247 ([Pa.] 2021) ("***Dunkins II***"), our Supreme Court concluded that a student's assent to his college's computing resources policy resulted in a voluntary relinquishment of any expectation of privacy concerning the records of his connection to the campus wireless internet network. [***See i***]***d***. at 255-56. This Court has held that an individual lacks a reasonable expectation of privacy over emails and chat room messages once those communications are received by the intended recipients because "once the [message] is received and opened, the destiny of the [message] then lies in the control of the recipient [ ], not the sender, absent some legal privilege." ***Commonwealth v. Proetto***, 771 A.2d 823, 83[1] (Pa. Super. 2001) (citation omitted), *aff['d]*, [] 837 A.2d 1163 ([Pa.] 2003). We have likewise held that, when an individual turns his computer in to a repair shop and the repair necessarily entail access to the video files stored on the computer, the individual "has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents." ***Commonwealth v. Sodomsky***, 939 A.2d 363, 369 (Pa. Super. 2007).

Regarding IP addresses, the Third Circuit Court of Appeals has stated that "[f]ederal courts have uniformly held that" individuals do not have a cognizable privacy interest in their IP addresses. ***United States v. Christie***, 624 F.3d 558, 573 (3d

> Cir. 2010)[. ***S***]***ee also***, ***e.g.***, ***United States v. Trader***, 981 F.3d 961, 967-68 (11th Cir. 2020); ***United States v. Morel***, 922 F.3d 1, 9 (1st Cir. 2019); ***United States v. Contreras***, 905 F.3d 853, 857 (5th Cir. 2018). As that court explained, "no reasonable expectation of privacy exists in an IP address, because that information is . . . not merely passively conveyed through third party equipment, but rather [ ] voluntarily turned over [to internet service providers] in order to direct the third party's servers." ***Christie***, 624 F.3d at 574 (citation omitted).

Kurtz, 294 A.3d at 520–21 (footnote omitted).[4]

Turning to the matter before us, Zealor argues the administrative subpoenas, issued pursuant to section 5743.1, are constitutionally infirm because they were not "limited to subscriber information." Zealor's Brief at 13. Specifically, Zealor argues that the collection of "payment information and internet connection logs requested by both administrative subpoenas as well as the search of the internet connection logs for each port associated with [his] IP address" should be deemed constitutionally protected as was the information in, *e.g.*, ***Carpenter v. United States***, 585 U.S. 296 (2018).[5]

---

[4] Our Supreme Court later affirmed this Court's decision in ***Kurtz***. A plurality of the Supreme Court affirmed this Court's conclusion that Kurtz lacked a reasonable expectation of privacy in his IP address; however, three justices in a concurrence opined that they would have affirmed on other grounds and not reached this issue. ***See Kurtz***, 348 A.3d 133, 156 (Pa. 2025) (OAJC stating that Kurtz had no enforceable expectation of privacy in his internet searches); ***id***. at 156-57 (Todd, C.J., concurring). Justice Donohue dissented. ***See id***. at 163-64.

[5] In ***Carpenter***, the United States Supreme Court limited the application of the third-party doctrine in the context of a search of cell-site location information ("CSLI"), which is information that is collected and stored by wireless carriers when a user's cell phone connects to a specific radio antenna,
(Footnote Continued Next Page)

Following our review, we conclude Zealor's argument merits no relief. Here, Zealor develops no argument that his payment information extended to anything other than his name and address associated with the account number used to pay for service. To the extent Zealor suggests that his payment information is constitutionally protected, this Court has rejected this argument. ***See Kurtz***, 294 A.3d at 520 (noting that the Constitutional protections afforded to "substantive" bank records do not extend to basic account information).

Next, we address Zealor's argument as it pertains to his IP address connection logs. This Court has held that an individual lacks a reasonable expectation of privacy over emails and chat room messages because once the information is sent to the intended recipients, they are free to do what they like with the information, unless a legal privilege applies. ***See id***. at 521. This Court has likewise found persuasive authority from the Third Circuit Court of Appeals holding that individuals do not have a privacy interest in their IP addresses and internet searches, because the information is not passively

---

or cell site. ***See*** 585 U.S. at 300-01. However, the ***Carpenter*** decision rested on the fact that CSLI is "not truly 'shared' [with a third party] as one normally understands the term" because "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." ***Id***. at 2220. In addition, the Court noted that through the collection of CSLI, the government was able to build "a detailed chronicle of [the defendant's] physical presence compiled every day, every moment, over several years," that the defendant could "in no meaningful sense [have] voluntarily assume[d] the risk of turning over." ***Id***. (internal citation and quotations omitted).

conveyed but voluntarily turned over to the internet service providers in order to access the third party's servers. ***See id***. (discussing ***Christie***, 624 F.3d at 574). In ***Kurtz***, we distinguished the instant scenario from ***Carpenter***, which involved the collection of CSLI, because CSLI is passively conveyed by the mere powering on of a cell phone whereas each time an individual chooses to access another's server, the individual provides their IP address voluntarily; additionally, we note the period for which information was sought in ***Kurtz*** was for a discrete seven-day period and it was limited to searches involving the victim of Kurtz's crime. ***See*** 294 A.3d at 522-23.[6]

Here, the PSP downloaded child pornography, in this case video of the molestation of a two-to-four-year-old girl, from the IP address at issue herein. ***See*** N.T., 9/20/24, Ex. C-5 (Search Warrant), at 15. Based on this information, the Commonwealth issued an administrative subpoena on Comcast for this IP address and determined the subscriber information and

---

[6] Zealor argues our holding in ***Kurtz*** was dictum because there was a search warrant in that case. ***See*** Zealor's Brief at 15. However, Zealor is incorrect. The first rationale for our affirmance of the denial of suppression was that Kurtz did not have a reasonable expectation of privacy in his IP address. Only after that conclusion did we hold in the alternative that the warrant was supported by probable cause. ***See*** 294 A.3d at 522-23. ***See also Commonwealth v. Derby***, 678 A.2d 784, 788 (Pa. Super. 1996) (stating that "where a decision rests on two or more grounds, none can be relegated to the category of *obiter dictum*. . . . The fact that the same result may be reached by either of two rulings of a court does not make either dictum") (internal citation, brackets, and quotations omitted).

service address was for Digital Media, LLC, 1514 W. Marshall Street, with a billing address for Jefferson Apartments. ***See id***. at 16. Corporal Reppert spoke to a general manager at Digital Media, who informed him that Digital Media managed all of the internet connections at Jefferson Apartments, and that "customers share a ***singular public facing IP address*** and that connections are established through Network Address Translation," in this case, a "network gateway such as a router," with an "assigned port number" that each device can use to send and receive communications. ***Id***. (emphasis added). Thus, with a combination of the shared public facing IP address and a port number, a particular subscriber can be identified. ***See id***.

The Commonwealth subsequently issued an administrative subpoena to Digital Media LLC for, *inter alia*, router log information for users who made connections between the shared IP address at issue herein and forty-eight specific IP addresses associated with an "infohash"—*i.e.*, a unique identifier for a torrent file (*i.e.*, a file used to convey a file or group of files *via* torrent software)[7]—linked to torrents for the distribution of child pornography. ***See*** N.T., 9/20/24, Ex. C-5 (Search Warrant), at 17; ***see also id***., C-4 (Administrative Subpoena on Digital Media LLC). Digital Media turned over to the Commonwealth router log information showing that the device utilizing the shared IP address and port number 58018 was associated with the child

[7] ***See*** N.T., 9/20/24, Ex. C-5 (Search Warrant), at 10.

pornography infohash discussed above. ***See id***. The router log information showed that Zealor was the subscriber using this port number. ***See id***.

Contrary to Zealor's suggestion that the subpoenas would allow the Commonwealth to create a "detailed picture" of his "personal affairs, opinions, habits," and "familial, political, professional, religious, and sexual associations," in contravention of ***Carpenter***, the subpoenas were limited to information about Zealor's connections, *via* his port and a shared public facing IP address, to other IP addresses associated with an infohash for a torrent containing, *inter alia*, a thirty-six second long video depicting a prepubescent girl (of approximately eight to ten years of age) receiving oral sex. ***See id***., Ex. C-5, at 17. Thus, as in ***Kurtz***, the information sought via the administrative subpoenas was not of the sort passively collected through the mere powering on or operation of Zealor's computer; rather, he took several affirmative steps, including using his router and port number and IP address to download a P2P sharing program, after which he chose to use his router and IP address to, using the P2P software, connect with other users *via* their IP addresses to share child pornography which contained identifiers (*i.e.*, the infohash) indicating it was child pornography. Zealor could have no reasonable expectation of privacy in the fact that he shared child pornography, indicated with a particular infohash, on a P2P program with third parties. ***See Kurtz***, 294 A.3d at 520–21. Notably, torrent files "are typically found as a [mere] result of keyword searches in internet sites that host or link them."

See N.T., 9/20/24, Ex. C-5 (Search Warrant), at 10.[8] Based on the foregoing, Zealor has failed to show the trial court erred in concluding he had not demonstrated a reasonable expectation of privacy, and, as such, neither the Fourth Amendment, nor Article I, Section 8, are implicated, ***see Enimpah***, 106 A.3d at 699, and Zealor's constitutional challenge fails.

In his second issue, Zealor argues the trial court erred in denying suppression because the subpoenas allowed the Commonwealth to obtain information beyond the scope permitted by section 5743.1. He maintains his "method of payment" and the IP address connection information are not listed in section 5743.1(a)(1)(ii) and, adds without development, that these are not the type of information the statute contemplates. Zealor's Brief at 17. Zealor suggests that this information goes beyond the "limited subscriber data" the statute addresses and instead shows the subpoenas were used "as an investigatory tool to review sensitive data without obtaining a warrant." ***Id***. at 18.

The trial court considered Zealor's argument and concluded it merits no relief, as "the information requested was either specifically authorized by the statute or encompassed in the provision permitting the Attorney General to obtain 'other subscriber number or identity, including any temporarily assigned network address, which may be relevant to an authorized law

---

[8] Additionally, we observe that Zealor does not assert that he took any steps to protect his privacy.

enforcement inquiry[.]'" Trial Court Opinion, 5/29/25, at 11 (quoting 18 Pa.C.S.A. § 5743.1(a)(1)(ii)(A)).

Assuming, *arguendo*, that the administrative subpoena in which the Commonwealth sought Zealor's method of payment and IP address connection log records were outside of the scope of section 5743.1(a)(1)(ii)(A), we conclude that Zealor is due no relief, as this violation of the statute would be non-constitutional, as discussed above, and, as such, suppression is an inappropriate remedy.[9] In ***Commonwealth v. Dougalewicz***, 113 A.3d 817, 826 (Pa. Super. 2015), this Court held that in the Act—which includes section 5743.1—"the Pennsylvania legislature excluded suppression as a remedy for non-constitutional violations . . .." ***Dougalewicz***, 113 A.3d at 826. Accordingly, Zealor's issue merits no relief.

In his third issue, Zealor argues the Commonwealth had no jurisdiction to serve administrative subpoenas to businesses outside of Pennsylvania, and, accordingly, suppression is warranted. ***See*** Zealor's Brief at 20. Zealor points to authority including, *inter alia*, Pennsylvania Rule of Criminal Procedure 200 for the principle that, with respect to search warrants, an issuing authority may only issue search warrants for the judicial district in which the authority

---

[9] While the trial court concluded the information sought did not exceed the scope of the statute, ***see*** Trial Court Opinion, 5/29/25, at 9, 11, 12, it is well settled that we may affirm the court's ruling on any legal basis. ***See Commonwealth v. Clouser***, 998 A.2d 656, 661 n.3 (Pa. Super. 2010).

and party are located. He also notes that 42 Pa.C.S.A. § 5964(a) provides that where a witness in another state is required for a criminal prosecution or grand jury investigations, the process required is that a judge of the court may issue a certificate stating the basis for requiring the witness's presence and the certificate shall be presented to a judge of a court in the jurisdiction where the witness is located. Because, Zealor maintains, section 5743.1(b)(3) contemplates service in this Commonwealth of an agent of the corporation, and service was not made in Pennsylvania, section 5964(a) applies, and the Commonwealth was required to issue the subpoenas in accordance with section 5964(a).

The trial court considered this argument and determined it merits no relief. The court noted that the Act specifically permits service of an administrative subpoena on a domestic or foreign corporation *via* an officer of the entity or a managing or general agent of the entity. ***See*** Trial Court Opinion, 5/29/25, at 13 (discussing section 5743.1(b)(3)). The court additionally observed that to compel compliance with the subpoena, the Commonwealth may invoke the aid of, *inter alia*, a court of common pleas in the "jurisdiction in which the subpoenaed person resides, or conducts business or may be found." ***Id***. at 13-14 (discussing section 5743.1(c)(1)). The court reasoned that that the statute thus authorizes administrative subpoenas on foreign companies, and, "[f]or each of the administrative subpoenas at issue in this case, both Comcast and Digital Media turned the requested information

over to Pennsylvania State Police. There was no need to take additional steps to enforce them." ***See id***. at 14.

Following our review, we likewise conclude Zealor is due no relief. Initially, we find Zealor's reliance on Pa.R.Crim.P. 200 and section 5964(a) to be misplaced, as the former pertains to search warrants, and the latter to compelling a witness for criminal proceedings. Neither speaks to the issue of administrative subpoenas, while section 5743.1 expressly addresses service of process on domestic and foreign entities; accordingly, there is no need for us to look to Rule 200 or section 5964(a).

Next, we observe that section 5743.1(b)(3)(i), (ii) permits service upon a foreign corporation by delivery of a subpoena to, *inter alia*, an officer of the entity or a managing or general agent of the entity. ***See*** 18 Pa.C.S.A. § 5743.1(b)(3)(i), (ii).[10] Nothing in these service provisions requires the person served to be in this Commonwealth. As is undisputed in this case, the DAG served the administrative subpoena on Comcast and Digital Media, after which Comcast and Digital Media complied with the subpoenas. Had the DAG

---

[10] We note that section 5743.1(b)(3)(iii) also permits service upon a foreign corporation by delivering a subpoena to an "agent authorized by appointment or by law to receive service of process in this Commonwealth." Subsection (iii) is the only one that mentions service of process on an authorized agent in Pennsylvania; therefore, had the legislature intended for service to be only on agents in Pennsylvania, it could have so specified for each of the subsections instead of just subsection (iii). The canon of statutory instruction, *expressio unius ist exclusio alterius*, supports this interpretation. ***See Thompson v. Thompson***, 223 A.3d 1272, 1277 (Pa. 2020).

needed judicial involvement in enforcing the subpoenas, it could have sought the assistance of a trial court in the jurisdictions where Comcast and Digital Media conduct business. ***See id***. at 5743.1(c)(1)(ii). However, it was unnecessary for the DAG to do so. Because the statute authorized service on Comcast and Digital Media, as foreign corporations, after which Comcast and Digital Media complied with the subpoenas without judicial intervention, Zealor's challenge is meritless.[11]

Judgment of sentence affirmed.

Judgment Entered.

Benjamin D. Kohler

Benjamin D. Kohler, Esq.
Prothonotary

Date: 4/22/2026

[11] We also reiterate that suppression is not a remedy for non-constitutional violations of the Act, and, so, even if Zealor's argument were correct, it would not merit suppression. ***See Dougalewicz***, 113 A.3d at 826.