2026 PA Super 209

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF PENNSYLVANIA
v.	:	
CLINTON M. THOMAS	:	
Appellant	:	No. 429 WDA 2025

Appeal from the Judgment of Sentence Entered March 12, 2025
In the Court of Common Pleas of Fayette County
Criminal Division at No: CP-26-CR-0001597-2023

BEFORE: LAZARUS, P.J., STABILE, J., and NEUMAN, J.

OPINION BY STABILE, J.: **FILED: September 21, 2026**

Appellant, Clinton M. Thomas, appeals from the judgment of sentence entered on March 12, 2025, by the Court of Common Pleas of Fayette County under which he was sentenced to an aggregate six to 12 years imprisonment for his convictions on the possession and dissemination of child sexual abuse material ("CSAM") and use of a communication facility to do so. He challenges the denial of his suppression motion and the admissibility and sufficiency of evidence. Upon review, we affirm Appellant's convictions for sexual abuse of children (possession),[1] and criminal use of a communication facility[2] but reverse his conviction for sexual abuse of children (dissemination)[3]. We therefore vacate the judgment of sentence, remand for resentencing on Counts 1-20, and 22, and grant a new trial on Count 21.

---

[1] 18 Pa.C.S.A. § 6312(d).

[2] 18 Pa.C.S.A. § 7512(a).

[3] 18 Pa.C.S.A. § 6312(c).

On August 18, 2023, Appellant was charged with 20 counts of sexual abuse of children (possession) and one count each of sexual abuse of children (dissemination) and criminal use of a communication facility. This matter originated when Google and Facebook reported CSAM to the National Center for Missing and Exploited Children[4] ("NCMEC") through NCMEC's CyberTipline[5]. The CyberTipline reports were sent from NCMEC to the Pennsylvania State Police ("PSP") via the Internet Crimes Against Children ("ICAC") network.[6] Upon receipt of this information, PSP Corporal Nathan Brown, the Coordinator of the Southwestern Pennsylvania Computer Crimes Unit, began an investigation.

The information in the CyberTipline reports contains, *inter alia*, usernames, e-mail addresses, telephone numbers, IP addresses, and identification of CSAM. N.T. Trial, 12/3/24, at 36. Based on this information,

---

[4] As more fully discussed, *infra,* "[t]he National Center for Missing & Exploited Children is a private, non-profit 501(c)(3) corporation whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization." ***See*** https://www.missingkids.org/footer/about.

[5] "NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet." ***See*** https://www.missingkids.org/gethelpnow/cybertipline#whathappenstoinformationinacybertip.

[6] NCMEC collects and analyzes digital reports of child exploitation, then routes those leads to regional ICAC task forces for local law enforcement investigation and arrests.

Corporal Brown issued an administrative subpoena to Verizon, the internet service provider in this case, to identify who owned the IP address on the dates and times contained within the CyberTipline reports. ***Id.*** at 37. Upon return of information under this subpoena, the physical address for Appellant was identified. ***Id.*** Corporal Brown used this information to apply for a search warrant for the property identified as Appellant's location. ***Id.*** at 38. The warrant allowed for the search and seizure of all electronically stored media or information, including all cell phone devices and computers. N.T. Suppression, 10/17/24, Commonwealth Exhibit 2.

Upon execution of the warrant, Appellant was found in the home. Several electronic devices were found and seized, including a white cell phone case, tablet, black and red cell phone case, a gray TCL Cricket phone, and a Samsung Android phone. N.T. Trial, 12/3/24, Commonwealth Exhibit 1. After the items were seized, Corporal Brown examined the devices for CSAM. He testified that CSAM was found on the Samsung and TCL cell phones. This evidence formed the basis for the criminal complaint and information filed against Appellant.

Appellant filed a motion to suppress all evidence seized as a result of what he maintained were unconstitutional warrantless searches by Facebook, Google, and NCMEC acting as government agents in violation of the Fourth Amendment and Article I, Section 8 of our Pennsylvania Constitution. The motion also sought to suppress any evidence obtained from Appellant's residence under the search warrant issued that was premised upon what

Appellant claimed was illegally seized evidence by Google, Facebook and NCMEC, as fruit of the poisonous tree. The motion was denied.

A jury trial was held on December 3, 2024, whereupon Appellant was convicted on all counts. Sentencing was deferred pending the assessment by the Sexual Offenders Assessment Board ("SOAB") to determine whether Appellant should be classified as a sexually violent predator ("SVP").

On March 12, 2025, Appellant was sentenced to an aggregate six to 12 years imprisonment. He was not classified as an SVP. Appellant filed a timely notice of appeal. Both the trial court and Appellant have complied with Pa.R.A.P. 1925. Appellant raises the following issues for our review:

> 1. Whether the suppression court committed reversible error by failing to suppress evidence that police obtained based on CyberTipline Reports by [NCMEC] where such evidence was obtained by means of a warrantless search of Appellant's electronic files maintained by Google and Facebook[.]
>
> 2. Whether the trial court committed reversible error by admitting testimony and evidence regarding the contents of the CyberTipline Reports into evidence over Appellant's objections based on hearsay and lack of foundation[.]
>
> 3. Whether the Commonwealth failed to present sufficient evidence to prove beyond a reasonable doubt that Appellant intentionally possessed child [sexual abuse material] or disseminated child [sexual abuse material] through a communication facility[.]

Appellant's Brief, at 3-4.

As Appellant's third issue challenging the sufficiency of the evidence, if meritorious, would result in discharge, we address that issue first. ***Commonwealth v. Koch***, 39 A.3d 996, 1001 (Pa. Super. 2011); ***see also***

Commonwealth v. Mullins, 918 A.2d 82, 85 (Pa. 2007) ("[t]he Double Jeopardy Clause bars retrial after a defendant's conviction has been overturned because of insufficient evidence.").

1. Sufficiency

Upon review of a sufficiency challenge, our standard of review is:

> whether viewing all the evidence admitted at trial in the light most favorable to the verdict winner, there is sufficient evidence to enable the fact-finder to find every element of the crime beyond a reasonable doubt. In applying the above test, we may not weigh the evidence and substitute our judgment for the fact-finder. In addition, we note that the facts and circumstances established by the Commonwealth need not preclude every possibility of innocence. Any doubts regarding a defendant's guilt may be resolved by the fact-finder unless the evidence is so weak and inconclusive that as a matter of law no probability of fact may be drawn from the combined circumstances. The Commonwealth may sustain its burden of proving every element of the crime beyond a reasonable doubt by means of wholly circumstantial evidence. Moreover, in applying the above test, the entire record must be evaluated and all evidence actually received must be considered. Finally, the finder of fact, while passing upon the credibility of witnesses and the weight of the evidence produced is free to believe all, part or none of the evidence.

Commonwealth v. Smith, 206 A.3d 551, 557 (Pa. Super. 2019) (citation omitted). In conducting a sufficiency review, we consider all evidence actually admitted at trial and do not review a diminished record. ***Id.*** Consequently, our sufficiency examination is unaffected by the subsequent resolution of any evidentiary issues raised by Appellant.

The entirety of Appellant's sufficiency arguments across all three offenses for which he was convicted is as follows:

> In this case, [Appellant] respectfully submits that [the] Commonwealth failed to present sufficient evidence that he violated [Child sexual abuse material], 18 Pa. C.S. § 6312(d) (20 counts); [Dissemination of photographs, videotapes, computer depictions and films] 18 Pa. C.S. § 6312(c) (one count); or Criminal Use of Communication Facility, 18 Pa. C.S. § 7512(a).
>
> In order to establish that [Appellant] was in possession of [CSAM] in violation of Section 6312(d), the Commonwealth must prove three elements beyond a reasonable doubt: 1) there must be a depiction of an actual child engaged in a prohibited sexual act or simulated sexual act; 2) the child depicted must be under the age of 18; and 3) defendant must have knowingly controlled and possessed the depiction. ***Commonwealth v. Colon-Plaza***, 136 A.3d 521, 52[6] (Pa. Super. 2016); ***Commonwealth v. Koehler***, 914 A.2d 427, 436 (Pa. Super. 2006). Similarly, to prove violations of Sections 6312(c) and Criminal Use of Communication Facility, the Commonwealth must prove beyond a reasonable doubt that [Appellant] knowingly and intentionally distributed, delivered, disseminated, transferred or displayed [CSAM] or that he used a communication for such purpose. 18 Pa. C.S. § 6312(c); ***Commonwealth v. Sauers***, 159 A. 3d 1 (Pa. Super. 2017)
>
> A review of the evidence and testimony submitted at trial demonstrates that the Commonwealth failed to prove beyond a reasonable doubt that [Appellant] knowingly possessed and controlled [CSAM]. Indeed, the Commonwealth did not produce any direct evidence that [Appellant] downloaded any of the [CSAM] images that the Commonwealth displayed to the jury at trial. Moreover, the Commonwealth failed to present sufficient evidence that [he] transmitted any of the images through a communication facility such as e-mail or social media.

Appellant's Brief, at 21-22.

The analysis provided under Appellant's sufficiency challenge, which he neatly compacts into a single paragraph, does not separately discuss the elements of each offense, but rather summarily argues that the evidence was

insufficient to establish that Appellant knowingly possessed CSAM, that he downloaded any CSAM images, and that he transmitted any images through a communication facility.[7] Absent from this analysis is discussion of any record evidence, and in particular, in a light most favorable to the Commonwealth as the verdict winner. ***Smith, supra.*** The trial court, nonetheless, discussed the record evidence on these sufficiency claims which we quote verbatim:

> The testimony of Corporal Brown alone satisfies all three [] elements. Corporal Brown found images of exposed children under the age of 18, and some engaged in sexual acts. These images were published to the members of the jury during the Commonwealth's case-in-chief. Corporal Brown found these images on the two cell phones found within Appellant's control. Further, the phones were examined for dissemination, discussed further below, wherein the [CSAM] were found to have been sent using Facebook and Google, solidifying that the Appellant had knowledge of the possession of these depictions.
>
> For these reasons, the Commonwealth has provided sufficient evidence to prove beyond a reasonable doubt that Appellant possessed [CSAM].
>
> Under 18 Pa.C.S.A. § 6312(c), a person is guilty of disseminating photo/films of child sex acts when he "[K]nowingly sells, distributes, delivers, disseminates, transfers, displays or exhibits to others, or who possesses for the purpose of sale, distribution, delivery, dissemination, transfer, display or exhibition to others,

---

[7] We note that we could find waiver of the sufficiency claim because Appellant failed to specify the element or elements challenged in his Rule 1925(b) statement. ***See Commonwealth v. McFarland***, 278 A.3d 369, 381 (Pa. Super. 2022) (citation omitted). Because Appellant specified the element challenged in his brief and the trial court addressed his sufficiency claims, we will decline to find waiver. ***See Commonwealth v. Martz***, 2022 WL 1698148 at *2 n.5 (Pa. Super. filed May 27, 2022) (unpublished memorandum).

> any child sexual abuse material or artificially generated child sexual abuse material."
>
> Here, Appellant was found with numerous photographs and depictions of [CSAM]. Corporal Brown testified that images were sent from Appellant's electronic device to an email out of the country. The image was distributed through Appellant's Facebook and corroborated as Appellant's account through his email address. This is sufficient to show that the Appellant knowingly disseminated [CSAM] to others.
>
> Under 18 Pa.C.S.A. § 7512(a), a person is guilty of criminal use of communication facility if "[T]hat person uses a communication facility to commit, cause or facilitate the commission or the attempt thereof of any crime which constitutes a felony under this title." The term "communication facility"' means a public or private instrumentality used or useful in the transmission of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part, including, but not limited to, telephone ... or ... mail. 18 Pa.C.S.A. § 7512(c).
>
> To support a conviction for criminal use of a communication facility under Section 7512, "the Commonwealth must prove beyond a reasonable doubt that: (1) [Appellant] knowingly and intentionally used a communication facility; (2) [Appellant] knowingly, intentionally or recklessly facilitated an underlying felony; and (3) the underlying felony occurred." ***Commonwealth v. Moss***, 852 A.2d 374, 382 (Pa. Super. 2004). "Facilitation" is "any use of a communication facility that makes easier the commission of the underlying felony." ***Id.***
>
> Here, Appellant knowingly and intentionally used his electronic device, the Samsung and/or TCL phone, to disseminate the images of [CSAM] through Facebook. The intentional use of Facebook through the use of a cellphone to disseminate images constitutes the facilitation of the felony. Lastly, the dissemination of [CSAM] is the underlying felony.

Trial Court Opinion, 6/11/25, at 7-9. We find the trial court's analysis and discussion of record evidence to dispose adequately of Appellant's sufficiency claims. We add that the record also was sufficient to convict under section

7512(a), in that Appellant used a communication device to facilitate the commission of a felony. By either uploading and/or downloading CSAM onto his cell phone(s), Appellant facilitated the commission of his felony possession convictions through a communication device. ***See Commonwealth v. Colon-Plaza***, 136 A.3d 521, 527-29 (Pa. Super. 2016) (evidence clearly sufficed to find Appellant guilty of all elements of section 7512(a) offense beyond a reasonable doubt where CSAM was downloaded and viewed on a laptop); ***Commonwealth v. Diodoro***, 970 A.2d 1100, 1103 n.3 (Pa. 2009) (accessing and viewing CSAM over the internet constitutes an offense under section 7512(a)). Appellant is not entitled to relief on this issue.

2. Suppression; The Private Actor Doctrine

Appellant argues that the trial court committed reversible error by failing to suppress any evidence received as the result of the warrantless searches conducted by Google, Facebook and/or NCMEC, who he contends were acting as agents of law enforcement and/or at the behest of law enforcement. Omnibus Pretrial Motion, 8/25/24, ¶¶ 21, 22. Appellant contends that the warrantless searches violated his rights under both the Fourth Amendment and Article I, Section 8 of our Pennsylvania Constitution.[8] ***Id.*** He also argues that any evidence obtained from his residence under the search warrant

[8] Since Pennsylvania case law follows federal precedent on this issue of "private actors", ***see Commonwealth v. Shaffer***, 209 A. 3d 957 (Pa. 2019), for convenience, our discussion when referencing the Fourth Amendment also subsumes application of this doctrine under Article 1, Section 8 of our Pennsylvania Constitution.

should have been suppressed as fruit of the poisonous tree because the warrant was premised upon the illegally seized evidence by Google, Facebook and NCMEC. ***Id.*** at ¶ 23.

Our standard of review when addressing a challenge to the denial of a suppression motion is

> limited to determining whether the factual findings are supported by the record and whether the legal conclusions drawn from those facts are correct. We are bound by the suppression court's factual findings so long as they are supported by the record; our standard of review on questions of law is *de novo*. Where, as here, the defendant is appealing the ruling of the suppression court, we may consider only the evidence of the Commonwealth and so much of the evidence for the defense as remains uncontradicted.

Commonwealth v. Yandamuri, 159 A.3d 503, 516 (Pa. 2017) (internal citations omitted). Moreover, our scope of review is limited to the record created during the suppression hearing. ***In re L.J.***, 79 A.3d 1073, 1085 (Pa. 2013).

The trial court made the following findings of fact following the suppression hearing:

> Corporal Nathan Brown, who has worked in the southwestern Pennsylvania computer crimes unit of the Pennsylvania State Police since 2008, reviewed three CyberTipline Reports dated May 18, 2023, May 20, 2023, and May 21, 2023. The reports had been sent to him by [NCMEC]. According to the Reports, NCMEC is a private, non-profit 501(c)(3) organization that serves as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. NCMEC had received information from Facebook (May 18, 2023 report) and Google (May 20, 2023 and May 21, 2023 reports) alerting it to possible [CSAM].

The Reports may be summarized as follows:

> (1) May 18, 2023 Report: based on information received from Facebook, there was an "incident" on May 15, 2023. The incident involved the chat service/IM client Messenger and occurred between [Appellant] and recipient Xavier Campeau in a chat room with the name "Xavier Campeau." The report indicated that a total of eleven (11) files were uploaded. The Report states on page 15 that NCMEC did not view the files.
>
> (2) May 20, 2023 Report: based on information received from Google, there was an "incident" on May 19, 2023, which the report indicates is the approximate date that Google became aware of the reported material. On page 31 of the report, it is stated that "Google became aware of the reported content which was stored in Google Photos infrastructure." The report indicated that fifty (50) files were uploaded. The Report states on page 63 that NCMEC viewed four (4) files.
>
> (3) May 21, 2023 Report: based on information received from Google, there was an "incident" on May 20, 2023, which the report indicates is the approximate date that Google became aware of the reported material. On page 31 of the report, it is stated that "Google became aware of the reported content which was stored in Google Photos infrastructure." The report indicated that two (2) files were uploaded. The Report states on page 46 that NCMEC did not view the files.

After receiving the CyberTipline reports, Corporal Brown viewed the images that had been forwarded to him. In his opinion, they met the definition of child [sexual abuse material], and he obtained administrative subpoenas for business records from Verizon and Google. Based on the information he received, he determined a relevant residential address and obtained a search

> warrant for various devices, hardware, and software applications at [Appellant's] residence and surrounding buildings or vehicles.

Trial Court Opinion, 11/6/24, at 1-3.

The Fourth Amendment to the United States Constitution and Article 1, Section 8 of the Pennsylvania Constitution protect citizens against unreasonable searches and seizures by law enforcement. ***See*** U.S. Const. amend. IV; Pa. Const. Art. I, § 8. "The proscriptions of the Fourth Amendment and Article I, § 8, do not apply to searches and seizures conducted by private individuals." ***Commonwealth v. Harris***, 817 A.2d 1033, 1047 (Pa. 2002). However, the Fourth Amendment does protect against searches or seizures conducted by a private party acting as an agent or instrument of the government. ***Commonwealth v. Yim***, 195 A.3d 922, 927 (Pa. Super. 2018) (citing ***Coolidge v. New Hampshire***, 403 U.S. 443 (1971)).

In ***Shaffer***, our Supreme Court examined the "private actor doctrine" as illustrated in the Supreme Court of the United States' seminal decision in ***United States v. Jacobsen***, 466 U.S. 109 (1984):

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

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

The High Court reversed, holding that "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as a result of private conduct." ***Jacobsen***, 466 U.S. at 126, 104 S.Ct. 165. The Court explained that "[t]o the extent that a protected possessory interest was infringed, the infringement was *de minimis* and constitutionally reasonable." ***Id.*** Acknowledging that the Fourth Amendment protects against both unreasonable searches and seizures, the Court defined a "search" as occurring "when an expectation of privacy that society is prepared to consider reasonable is infringed." ***Id.*** at 113, 104 S.Ct. 1652. It defined a "seizure" of property as occurring "when there is some meaningful interference with an individual's possessory interests in that property." ***Id.*** The Court proceeded to explain that this constitutional protection proscribed only governmental action and was wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official." ***Id.*** (citation omitted).

Categorizing the package as an "effect" in which an individual has a reasonable expectation of privacy, the Court observed that a warrantless search of the package would be presumptively unreasonable. ***Id.*** at 114, 104 S.Ct. 1652. However, the Court opined, "the fact that agents of the private carrier independently opened the package and made an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable." ***Id.*** at 114-15, 104 S.Ct. 1652. Accordingly, because the initial invasion of the package was accomplished by private action, the Court held that the Fourth Amendment was not violated, regardless of whether the private action was accidental, deliberate, reasonable, or unreasonable. ***Id.*** at 115, 104 S.Ct. 1652.

Significantly, the High Court explained that the additional invasions of privacy by the government agent "must be tested by the degree to which they exceeded the scope of the private search." ***Id.*** (citing ***Walter v. United States***, 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980)). The Court observed that "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." ***Id.*** at 117, 104 S.Ct. 1652. The High Court construed the governmental actions as twofold, first removing the contraband from its packaging and viewing it, and, second, conducting a chemical test of the powder. ***Id.*** at 118, 104 S.Ct. 1652.

Regarding the government agent's reopening of the package after having been told by the employees that it contained a white powder, the Court emphasized that "there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." ***Id.*** at 119, 104 S.Ct. 1652. As the government could use the employees' testimony regarding the contents of the package, the Court found that "it hardly infringed [the defendants'] privacy for the agents to re-examine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube." ***Id.*** The Court observed that this governmental action did not further infringe upon the defendants' privacy, but rather merely avoided the risk of a flaw in the employees' recollection. ***Id.*** The High Court held that the defendants "could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents." ***Id.*** It concluded that the DEA agent's observation of what a private party had voluntarily made available for his inspection did not violate the Fourth Amendment. ***Id.***

In the same vein, the Court ruled that the removal of the plastic bags from the tube and the visual inspection of the contents provided the agent with no more information than what had been discovered during the private search. Thus, the High Court opined, the agent's actions "infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment." ***Id.*** at 120, 104 S.Ct. 1652. Notably, the Court explained that while the agent's assertion of dominion and

> control over the package and its contents constituted a "seizure," the seizure was not unreasonable because the privacy interest in the package had already been compromised, as it had been opened and remained unsealed and because the agent had been specifically invited to examine the package's contents. ***Id.*** at 120-21, 104 S.Ct. 1652. The Court ruled that "since it was apparent that the tube and plastic bags contained contraband and little else, this warrantless seizure was reasonable, for it is well settled that it is constitutionally reasonable for law enforcement officials to seize 'effects' that cannot support a justifiable expectation of privacy without a warrant, based on probable cause to believe they contain contraband." ***Id.*** at 121-22, 104 S.Ct. 1652.
>
> The High Court proceeded to examine whether the agent's additional intrusion, occasioned by the field test of the white powder, exceeded the scope of the private search. The Court answered this inquiry in the negative, finding that the chemical test that merely disclosed whether a substance is cocaine did not compromise any legitimate interest in privacy as one cannot legitimately have a privacy interest in cocaine, an illegal substance. ***Id.*** at 123, 104 S.Ct. 1652. The Court concluded that because only a trace amount of the material was involved and because the property had been lawfully detained, "the 'seizure' could, at most, have only a *de minimis* impact on any protected property interest." ***Id.*** at 125, 104 S.Ct. 1652. Because the safeguards of a warrant would only minimally advance Fourth Amendment interests, the court concluded that the warrantless "seizure" was reasonable. ***Id.***

Shaffer, 209 A.3d at 969-971. Rejecting the appellant's suggestion otherwise, the Court iterated that there is ample support for the private search doctrine in Pennsylvania jurisprudence and that "[t]he proscriptions of the Fourth Amendment and Article I, § 8, do not apply to searches and seizures conducted by private individuals." ***Id.*** (citing ***Commonwealth v. Harris***, 817 A.2d 1033, 1047 (Pa. 2002)). The Court then held that "[p]ursuant to ***Jacobsen***, our inquiry is two-fold: (1) whether the facts presented

establish that a private search was conducted; and, if so, (2) whether the police actions exceeded the scope of the private search." ***Id.*** at 972.

There are however two circumstances where the private actor doctrine does not apply. "First, the doctrine does not apply if the 'private actor' who conducted the search was actually an agent or instrument of the government when the search was conducted." ***United States v. Meals***, 21 F.4th 903, 906 (5th Cir. 2021). Second, if without a warrant, the government "exceeds the scope of the private actor's original search and discovers new evidence that it was not substantially certain to discover, the private search doctrine does not apply, and the new evidence may be suppressed."[9] ***Id.*** at 906. Therefore, unless one of the above-mentioned circumstances is present, "if a non-government entity violates a person's privacy . . . and turns over the evidence to the government, the evidence can be used to obtain warrants or to prosecute." ***Id.*** This is because the Fourth Amendment restrains the government, not private citizens. ***Id.***

"Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved 'in light of all the circumstances.'" ***Skinner v. Railway Labor Executives' Ass'n***, 489 U.S. 602, 614 (1989)

[9] Appellant does not assert that either NCMEC or the PSP exceeded the scope of the searches performed by Google and/or Facebook.

(citations omitted). The principles that guide us in this regard were first established by the Supreme Court of the United States in ***Lugar v. Edmondson Oil Co., Inc***, 457 U.S. 922 (1982), wherein the Supreme Court "held that the conduct allegedly causing the deprivation must be fairly attributable to the state." ***Yim***, 195 A.3d at 927 (citing ***Commonwealth v. Price***, 672 A.2d 280, 283-84 (Pa. 1996)). "[T]he critical factor is whether the private individual, considering all the circumstances of the case, must be regarded as having acted as an instrument or agent of the state[.]" ***Commonwealth v. Cieri***, 499 A.2d 317 (Pa. 1985) (cleaned up; citations omitted). Mere cooperation with police, however, does not transform private action into state action. ***Price,*** 672 A.2d at 283-284. Likewise, "the mere fact that police and prosecutors use the results of an individual's actions does not, alone, elevate those actions to state action." ***Id.*** "Where, however, the relationship between the person committing wrongful acts and the State is such that those acts can be viewed as emanating from the authority of the State, a finding of state action is warranted." ***Id.***

Appellant's challenge to the items seized by Google and Facebook and subsequently received by NCMEC, requires that we first determine whether, under the circumstances in this case, any of these entities were operating as "private actors" or instead, as "agents" or "instruments" of the government for Fourth Amendment purposes.

Appellant sought suppression of all evidence obtained by Corporal Brown based on the CyberTipline reports that were the product of the warrantless searches of Appellant's files by Google and Facebook and sent to NCMEC, as well as all evidence obtained under the search warrant issued to Corporal Brown under which Appellant claims his electronic devices were seized as fruit of the poisonous tree. ***See*** Appellant's Brief, at 13. Appellant argues that Corporal Brown acknowledged in his search warrant application that he received and reviewed information from NCMEC which NCMEC in turn received from Facebook and from Appellant's Internet service provider. ***See id.***

Appellant points to Corporal Brown's testimony wherein he stated that Google and Facebook identify and report child sexual abuse imagery in accordance with the federal statutory definition of CSAM as referenced in 18 U.S.C.A. § 2256, and that when possible danger is observed, a summary is sent to NCMEC CyberTipline. ***See id.*** at 14. Appellant sets forth that electronic service providers (ESPs) such as Google and Facebook must report any known CSAM violations to NCMEC, and that the failure to do so can be met with substantial criminal penalties. ***See id.*** at 17.

The suppression record confirms that Corporal Brown identified Appellant through the reports received from NCMEC based on information provided by Google and Facebook. Appellant admits there is no dispute that NCMEC provided inculpatory images/videos purportedly depicting unlawful

CSAM to law enforcement through four CyberTipline reports. Appellant points out that it was only after Corporeal Brown viewed images that were provided to him by NCMEC that he then requested search warrants.

While acknowledging that neither the Fourth Amendment nor Article I, § 8 apply to actions by private actors, Appellant argues, relying for the most part upon our unpublished decision in ***Commonwealth v. Baez***, 2021 WL 5626366, (Pa. Super. filed Dec. 1, 2021) (unpublished memorandum), that we must find that Google, Facebook and NCMEC were acting as agents of law enforcement in this case.

In addition, Appellant cites federal statutory law to establish that Google, Facebook and NCMEC are government actors. Appellant cites to 18 U.S.C.A. § 2258A,[10] without identifying the portion(s) of the statutory text relied upon, to establish that Google, Facebook and NCMEC must be deemed government actors. He broadly contends that Facebook and Google must be deemed government actors because by law they are mandated reporters and can face criminal penalties for failing to comply with their reporting obligations. Appellant is less specific as to NCMEC, but it is clear that his contention is that NCMEC also is a government actor as it too is bound by

[10] Section 2258A is a part of Chapter 110 of Part I of Title 18 of the United States Code (18 U.S.C. §§ 2251–2260A), titled "Sexual Exploitation and Other Abuse of Children."

federal law to report CSAM to law enforcement. We discern the pertinent provisions of § 2258A that underlie Appellant's argument to be the following:

> (a) Duty To Report.—
>
> (1) In general.—
>
> (A) Duty.— In order to reduce the proliferation of online child sexual exploitation and to prevent the online sexual exploitation of children, a provider[11]—
>
> (i) shall, as soon as reasonably possible after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(A) [apparent violation], take the actions described in subparagraph (B); and
>
> (ii) may, after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(B) [imminent violation], take the actions described in subparagraph (B).
>
> (B) Actions described.—The actions described in this subparagraph are—
>
> (i) providing to the CyberTipline of NCMEC, or any successor to the CyberTipline operated by NCMEC, the mailing address, telephone number, facsimile number, electronic mailing address of, and individual point of contact for, such provider; and
>
> (ii) making a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by NCMEC.
>
> * * * *
>
> (e) Failure To Report.—A provider that knowingly and willfully fails to make a report required under subsection (a)(1) shall be fined—

[11] A "provider" as used in this section "means an electronic communication service provider or remote computing service." 18 U.S.C.A. § 2258E(6).

> (1) in the case of an initial knowing and willful failure to make a report, not more than $850,000 in the case of a provider with not less than 100,000,000 monthly active users or $600,000 in the case of a provider with less than 100,000,000 monthly active users; and
>
> (2) in the case of any second or subsequent knowing and willful failure to make a report, not more than $1,000,000 in the case of a provider with not less than 100,000,000 monthly active users or $850,000 in the case of a provider with less than 100,000,000 monthly active users.

18 U.S.C.A. § 2558A(a), (e).

Although not discussed by Appellant, we observe, as the trial court did, that § 2558A also provides:

> (f) Protection of Privacy.—Nothing in this section shall be construed to require a provider to—
>
> (1) monitor any user, subscriber, or customer of that provider;
>
> (2) monitor the content of any communication of any person described in paragraph (1); or
>
> (3) affirmatively search, screen, or scan for facts or circumstances described in sections (a) and (b).

18 U.S.C.A. § 2258A(f).

Instantly, the trial court found that neither Facebook nor Google were acting as government agents reasoning as follows:

> Facebook and Google only were required to report to NCMEC facts and circumstances known to them; they were not required to supply any images or communications. They also were not required to "affirmatively search" for contraband. Therefore, it cannot be said that Facebook or Google were acting as government agents or at the request of a government entity. Instead, they were private actors that proactively identified images they suspected were contraband and then

> voluntarily forwarded those images to NCMEC with their reports.

Trial Court Opinion, 11/6/24, at 5. We agree.

Neither Facebook nor Google were required or requested by the government to search Appellant's account to locate CSAM. Section 2558A only mandates that they report any CSAM they may find. The mechanisms used to locate CSAM and the extent to which they conduct any search is left to the discretion of both Google and Facebook. They exercise their rights to regulate the content on their platforms and have put systems in place that find and flag content that includes CSAM. At no point did the government force them into the creation of this system. Nor does the record support any finding that Google and Facebook conducted their searches of Appellant's files at the government's urging or by any means of manipulation or coercion.

ESPs such as Google and Facebook are required under § 2558A to report any known CSAM to NCMEC, who in turn is required to send the report(s) to the local law enforcement agency (which it does through ICAC) where the CSAM is either downloaded or uploaded. Critically, this same law specifically disclaims any obligation by ESPs to monitor a) any user, subscriber, or customer of that provider, b) the content of any communication, or c) to affirmatively search, screen, or scan for CSAM. 18 Pa.C.S.A. § 2558(A)(f). Thus, the statute effectively places any decision to search within the discretion of the ESPs. ***See, e.g., United States v. Meals***, 21 F.4th 903 (5th Cir. 2021) (holding that nothing in the language under 2558A compelled or coerced ESPs

to *search* actively for evidence of CSAM). Accordingly, neither Facebook nor Google can be deemed government agents, even if the result of their searches benefits the government. ***Id.*** at 908; ***United States v. Miller***, 982 F.3d 412, 421-26 (6th Cir. 2020) (same); ***United States v. Ringland***, 966 F.3d 731 (8th Cir. 2020) (same); ***United States v. Rosenow***, 50 F.4th 715, 729-31 (9th Cir. 2022) ("federal law did not transform Yahoo's and Facebook's private searches into governmental action."); ***U.S. v. Cameron***, 699 F.3d 621, 637-38 (1st Cir. 2012) ("We will not find that a private party has acted as an agent of the government 'simply because the government has a stake in the outcome of the search.'"). Therefore, we too, like the trial court, conclude that neither Google nor Facebook were acting as government agents such that their searches ran afoul of the protections under the Fourth Amendment. Instead, the record here only supports the conclusion that they were at all times acting as "private actors."

Separately, Appellant also contends that the items received by NCMEC from Facebook and Google must be suppressed since NCMEC is a government actor. Appellant does not develop this argument in his brief beyond referring to the same statutory basis upon which he argued that Google and Facebook were government actors - § 2558A.

NCMEC "is a private, non-profit 501(c)(3) organization created in 1984 by child advocates to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public

on missing and sexually exploited child issues." ***See*** N.T. Suppression Hearing, 10/17/24, Exhibits 3-5 (CyberTipline Reports). Although NCMEC began as a non-profit organization, Congress has since empowered NCMEC to exercise significant law enforcement responsibility. The Administrator of the Office of Juvenile Justice and Delinquency Prevention is statutorily obligated to make an annual grant to NCMEC. 34 U.S.C.A. § 11293(b)(1). Monies from the grant shall be used to "work with families, law enforcement agencies, [ESPs], electronic payment service provides, technology companies, nongovernmental organizations, and others on methods to reduce the existence and distribution of online images and videos of sexually exploited children by operating a CyberTipline[.]" 34 U.S.C.A. § 11293(b)(1)(K)(i). The statute also provides that the grant money shall be used to "make reports received through the CyberTipline available to the appropriate law enforcement agency for its review and potential investigation[.]" 34 U.S.C.A. § 11293(b)(1)(K)(i)(II).

NCMEC's CyberTipline functions illustrate the special law enforcement duties and powers it enjoys. As explained, NCMEC is statutorily required to maintain an electronic tipline for ESPs and others to report apparent CSAM. ESPs must report any known CSAM to NCMEC via its CyberTipline, not to a law enforcement agency. 18 U.S.C.A. § 2258A(a)(1). Once NCMEC receives a report from an ESP, it is statutorily obligated to forward the report to federal, state, and/or local law enforcement agencies. 18 U.S.C.A. § 2258A(c). Thus,

NCMEC is statutorily authorized to receive and distribute CSAM, an action that would normally subject private citizens to criminal prosecutions. 18 U.S.C.A. § 2258A(a) (mandating ESP's report apparent CSAM to NCMEC's CyberTipline), (b)(4) (requiring visual depictions of apparent CSAM in the report to NCMEC), (c) (NCMEC required to forward reports of apparent CSAM to law enforcement). In addition to this authority, Congress has provided NCMEC with statutory immunity for civil and criminal prosecution "arising from the performance of the CyberTipline responsibilities or functions of NCMEC[.]" 18 U.S.C.A. § 2258D.

For present purposes, we need not resolve whether NCMEC was acting as a government agent, since there is no suggestion in the suppression record that NCMEC exceeded the scope of the private actor searches forwarded to it by Google and/or Facebook. ***Meals, supra.*** So long as NCMEC, and thereafter the police, did not exceed the searches conducted by the ESPs, those searches could be used by the government without transgressing Fourth Amendment protections. Accordingly, the trial court was correct to deny suppression based upon the searches possessed by NCMEC and thereafter forwarded to law enforcement.[12]

[12] Some circuit courts that have analyzed whether NCMEC acts as an instrument or agent of the government have concluded that NCMEC does function as an instrument or agent of the government. ***See United States v. Guard***, 152 F.4th 375, 387-89 (2d Cir. 2025); ***United States v. Ackerman***, 831 F.3d 1292, 1295-1300 (10th Cir. 2016).

Appellant's reliance upon our unpublished decision in ***Baez*** to argue that Facebook, Google and NCMEC were acting as agents of law enforcement is unavailing. The case is clearly distinguishable.

In ***Baez***, police officers responded to Baez's 911 call that someone had stolen his backpack at a Burger King. Officers arrived, located the backpack, and returned it to Baez. In the process, officers found that Baez had an open warrant out of Florida and/or a Monroe County probation detainer lodged against him. When Baez's friend, Christine Monaco, arrived to give him a ride, he gave her his backpack and requested she put it in her car. As it turned out, Ms. Monaco was friends with one of the responding officers. She asked the officer if she was allowed to put the backpack in her car. The officer told her that "he might be concerned about what [the backpack] could contain, explaining that Baez had previously been convicted for a firearm possession charge." ***Baez***, 2021 WL 5626366 at *1. "He asked her, 'Are you taking possession of the bag? . . . Do you want to check what's in it before you take possession of it?'" ***Id.*** "Ms. Monaco recalled him asking if she minded searching the backpack 'for her own protection, because, if she got pulled over, and there's something in the bag, it's going to be her responsibility.'" ***Id.*** Reaching in the backpack, she immediately felt a handgun and gave the bag to the police. The officers then searched through the contents, which included a clear baggie of suspected heroin.

The Commonwealth charged Baez with carrying a firearm without a license, possessing a firearm with an altered serial number, and various drug offenses. Baez subsequently moved to suppress the evidence against him upon the basis that when Ms. Monaco searched inside his backpack, she was acting as an agent of the state. The suppression court found that the Commonwealth did not prove Ms. Monaco acted entirely as a private individual. The court observed that Ms. Monaco asked for the officer's permission to take the backpack from the scene. From this, the suppression court reasonably inferred that Ms. Monaco believed herself to be under some amount of governmental control in this situation and that the officer created the situation that induced Ms. Monaco to search the backpack. Suppression was granted and we affirmed.

Notwithstanding the officer's suggested intent to protect Ms. Monaco from possible negative ramifications of transporting the backpack, on appeal, we held that the officer's actions directly caused Ms. Monaco to search the backpack, something the officer could not do without a search warrant. ***Id.*** at *5. We found that specific features of the officer's conduct combined to convince us that the officer did more than adopt a passive position toward the underlying private conduct. ***Id.***

The facts in ***Baez*** stand in stark contrast to those presently before us. ***Baez*** was illustrative of a situation where police manipulated and encouraged a private party to conduct a warrantless search. They were an active part of

the search coming into being. Here, the same cannot be said with respect to Facebook and Google whose searches were the product of their own policies and who were under no compulsion or urging by the police to search Appellant's internet files for CSAM.[13] ***Baez*** offers no quarter to Appellant. The trial court correctly denied suppression.

2. Hearsay; the Business Records Exception

In his last issue, Appellant contends the trial court committed reversible error in admitting a NCMEC CyberTipline report[14], Commonwealth Exhibit 2, into evidence through the testimony of Corporal Brown under the business records exception to hearsay under Pa.R.E. 803(6).[15] He seeks a new trial based upon this evidentiary error.

---

[13] We need not distinguish ***Baez*** from Appellant's claim that NCMEC was acting as a government agent, since we have concluded that Google and Facebook were not acting as government agents and NCMEC, even if acting as a government agent, did not exceed the scope of those private actor searches.

[14] As we discuss, *infra,* although multiple CyberTipline reports were admitted during the suppression hearing, only CyberTipline report 162402735, marked as Commonwealth Exhibit 2, was used and admitted into evidence during trial. Therefore, we limit our discussion on this hearsay issue to Commonwealth Exhibit 2.

[15] This exception to the rule against hearsay is codified at 42 Pa.C.S.A. § 6108, that provides as follows:

> **§ 6108. Business records.**
>
> **(a) Short title of section.--**This section shall be known and may be cited as the "Uniform Business Records as Evidence Act."

(Footnote Continued Next Page)

At trial, the Commonwealth, over objection, was permitted to introduce the CyberTipline report received from NCMEC through the testimony of Corporal Brown. The defense objected on the basis that Corporal Brown was not a "qualified" witness to admit the CyberTipline report as a business record. Appellant argues Corporal Brown was not a "qualified" witness to admit the record, since he is not employed by NCMEC, there was no testimony presented that he is the NCMEC custodian of records, or that he had personal knowledge of NCMEC's internal procedures with respect to recordkeeping. ***See*** Appellant's Brief, at 18-19. The trial court overruled the objection, explaining more fully in its 1925(a) opinion, that the records were admitted under the business records exception because:

> Here, Corporal Brown testified as to his complete familiarity with [CyberTipline] reports. Corporal Brown testified that these reports are received and used on a daily basis from NCMEC and ICAC, and that through his employment with the Computer Crimes Unit of the Pennsylvania State Police he has received twenty to thirty thousand of such [CyberTipline] reports. He relies on the information from the [reports] to conduct his investigation. Through this questioning, the trial court was satisfied that

---

> **(b) General rule.--**A record of an act, condition or event shall, insofar as relevant, be competent evidence if the custodian or other qualified witness testifies to its identity and the mode of its preparation, and if it was made in the regular course of business at or near the time of the act, condition or event, and if, in the opinion of the tribunal, the sources of information, method and time of preparation were such as to justify its admission.
>
> **(c) Definition.--**As used in this section "business" includes every kind of business, profession, occupation, calling, or operation of institutions whether carried on for profit or not.

> Corporal Brown relies on this business record from NCMEC or ICAC on a regular basis in conducting his investigations into [CSAM].

Trial Court Opinion, 6/11/25, at 5.

The admission or exclusion of evidence is within the sound discretion of the trial court. "[I]n reviewing a challenge to the admissibility of evidence, we will only reverse a ruling by a trial court upon a showing that it abused its discretion or committed an error of law." ***McManamon v. Washko****,* 906 A.2d 1259, 1268-69 (Pa. Super. 2006) (citation omitted). Thus, our standard of review is very narrow. "To constitute reversible error, an evidentiary ruling must not only be erroneous, but also harmful or prejudicial to the complaining party." ***Id.***

Herein, we are asked to review the trial court's admission of hearsay evidence. Hearsay is an out-of-court statement offered for the truth of the matter asserted and is generally inadmissible unless it falls within a delineated exception. ***See*** Pa.R.E. 801, 802. Records of a regularly conducted business activity are one such exception if admitted through a properly qualified witness. Pa.R.E. 803(6), the business records exception to the rule against hearsay, provides as follows:

> **(6) Records of a Regularly Conducted Activity.** A record (which includes a memorandum, report, or data compilation in any form) of an act, event, or condition if:
>
> (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;

> (B) the record was kept in the course of a regularly conducted activity of a "business", which term includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit;
>
> (C) making the record was a regular practice of that activity;
>
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and
>
> (E) the opponent does not show that the source of the information or other circumstances indicate a lack of trustworthiness.

Pa.R.E. 803(6). Central to laying a proper foundation for the admission of business records under this exception is that a custodian or other qualified witness testify to the identity of the records, the mode of their preparation, and if they were made in the regular course of business at or near the time of the act, condition or event. 42 Pa.C.S.A. § 6108.

However, even though a proper records custodian may adequately lay the foundation to admit business records as an exception to hearsay, admitting business records under this exception may not suffice to admit other hearsay within the records. "An out-of-court declaration containing another out-of-court declaration is double hearsay." ***Commonwealth v. Laich***, 777 A.2d 1057, 1060 (Pa. 2001). For double hearsay to be admissible, "the reliability and trustworthiness of each declarant must be independently established." ***Id.*** "This requirement is satisfied when each statement comes within an exception to the hearsay rule." ***Id.*** When attempting to admit

records that contain multiple layers of hearsay under the business records exception, each layer must qualify as an exception to the rule against hearsay for the ultimate records to be admitted. ***Id.***

Before further addressing this hearsay issue, we find that two aspects of the record deserve mention before proceeding to the merits of this issue.

First, it is not at all clear from a review of the record and the briefs if the Commonwealth, through the testimony of Corporal Brown, was attempting to admit the CyberTipline report as a business record of the PSP, or as a business record of NCMEC. In either event, as we discuss, *infra*, Corporal Brown's testimony was not adequate to admit Exhibit 2 as either a PSP or NCMEC business record.

Second, at trial, unlike during the pre-trial suppression hearing, only a single CyberTipline report, Exhibit 2,[16] was introduced into evidence.[17] Exhibit 2 is a 16-page PSP "General Offense Report" that contains the CyberTipline report from Facebook. The cover page on the PSP report contains an "Executive Summary" that provides a brief overview of information contained in the CyberTipline report. The CyberTipline report is broken down into four

---

[16] From our review of the certified record, trial Exhibit 2 corresponds to Exhibit 4 from the suppression hearing.

[17] At the suppression hearing, a total of six exhibits were introduced into evidence, three of which (Exhibits 3, 4, and 5) contained four (4) CyberTipline reports. Exhibits 3 and 5 identified three Google CyberTipline reports (Exhibit 3 contained two reports). Exhibit 4 identified Facebook as the CyberTipline reporter.

sections, A, B, C and D. Section "A" contains the original information received from Facebook, except for the "Incident Type" and "Incident Time" identified in that section. It identifies Appellant as the suspect, as well as "Xavier Campeau" as the recipient. Also identified are 11 uploaded files. The section concludes with a disclosure that all information in that section was electronically submitted to the CyberTipline by the reporting person, the NCMEC center or the reporting ESP. The information received is from the original submission. All information, other than the incident type and incident time, is voluntary and undertaken at the initiative of the reporting person or reporting ESP.

Section "B" contains "Automated Information Added by NCMEC Systems." When the reporting party voluntarily reports an IP address or phone number, NCMEC will geographically resolve the IP address or number via publicly available online queries. The data is approximate and may not display a user's exact location. The section also contains identification of a categorization system used by various ESPs that identify the type of CSAM material contained within the uploaded files. There finally is a "deconfliction" provision whereby NCMEC reports on automated queries on reports from section "A" to provide a list of possibly related results at the time the report was generated. The reported information attempts to match information seen in additional CyberTipline reports.

Section "C" is "Additional Information Provided by NCMEC." The section contains information collected by NCMEC staff based upon information electronically submitted by the reporting person, NCMEC call center or reporting ESP. The section may contain a variety of additional information, including data gathered from queries on publicly available, open-source websites. Queries conducted by NCMEC staff are documented and any query results are saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to the report. Section "C" to Exhibit 2 states that NCMEC did not view the 11 uploaded files and therefore has no information containing the content of the files other than the information voluntarily provided by the reporting ESP noted in the report.

As is plainly obvious, Exhibit 2 contains multiple layers of hearsay. The PSP record, even assuming it could be admitted as a business record, contains hearsay from NCMEC which in turn reported on hearsay supplied by Facebook. Exhibit 2 also identifies information from other sources that arguably might constitute other hearsay unless proper foundations are laid for their admission.[18] Some of the information also is from public sources that cannot be verified and which may constitute inadmissible hearsay as well.

---

[18] As stated earlier, NCMEC forwards its CyberTipline reports to police through ICAC. None of the parties or the trial court have commented on whether ICAC
(Footnote Continued Next Page)

If Corporal Brown was attempting to admit Exhibit 2 as a PSP record, he not only had to lay the proper foundation for admission of the PSP record, but he, if he was a qualified witness, also had to lay proper foundations for the NCMEC and ESP information contained within Exhibit 2 to be admitted under Pa.R.E. 802(6). If Corporal Brown was attempting to admit the CyberTipline report as a business record of NCMEC, in addition to establishing that he could qualify as a proper witness to do so, he still would have had to lay a proper foundation to admit the hearsay Facebook records within the NCMEC report to satisfy Pa.R.E. 802(6). At a minimum, Exhibit 2 contained as little as two and as many as three (and perhaps more) layers of hearsay, with each having to be properly authenticated under the business records exception for the entire exhibit to come into evidence.

While admittedly, as recognized by the trial court, Corporal Brown was very familiar with NCMEC CyberTipline reports and relies upon them in conducting CSAM investigations, this is not testimony that meets the criteria to admit a business record(s) under the hearsay exception under Rule 802(6). As stated, the rule requires that the *custodian of the record or another qualified witness*, testify that the record was made at or near the time the information was transmitted by someone with knowledge, that it was kept in the course of a regularly conducted activity of a business, and that making

---

factors into this hearsay analysis. Neither do we, limiting ourselves to the arguments presented.

the record was a regular practice of the business. No foundation was laid by the Commonwealth to qualify Corporal Brown as a proper witness to establish the bona fides of Exhibit 2 as a PSP business record, nonetheless as a qualified witness to testify as to either NCMEC's or Facebook's records.

Corporal Brown was not employed by NCMEC and has no first-hand familiarity with NCMEC's policies and practices with respect to its business records. The mere fact that he uses and relies upon NCMEC records in his investigations does not qualify him as a custodian or other qualified person to lay the foundation to admit NCMEC's business records into evidence, nonetheless those of the ESPs. In fact, no attempt was made to have Corporal Brown testify as a qualifying witness to admit the information reported by Facebook that was a part of the NCMEC CyberTipline report. Any attempt to admit Exhibit 2 had to be done through a qualified person(s) to provide the proper foundation to admit each level of hearsay. While a certification under

Pa.R.E. 902(11)[19] and (13)[20] may be used to self-authenticate[21] a record of a regularly conducted business or those of an electronic process or system, respectively, any attempt to satisfy a hearsay exception still must be made independently. ***See*** Comment to Pa.R.E. 902. It therefore was error for the trial court to admit Exhibit 2 as a business record through the testimony of Corporal Brown.[22]

---

[19] Pa.R.E. 902 allows for the admission of evidence that is self-authenticating and provides that:

> The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with Pa.R.C[iv].P. No. 76. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record – and must make the record and certification available for inspection – so that the party has a fair opportunity to challenge them.

Pa.R.E. 902(11).

[20] Pa.R.E. 902(13) speaks to records generated by an electronic process or system and provides:

> A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

[21] "[T]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it to be." Pa.R.E. 901.

[22] The realities of today's modern world have long passed beyond the days of when a single shopkeeper could testify to its business records without concern as to the incorporation of third-party records as a part of their own. Today, it
(Footnote Continued Next Page)

Having determined that it was error for the trial court to admit Exhibit 2 under the business records exception to the prohibition against hearsay, we now turn our attention to examining whether the error was harmless and if so, whether Appellant is entitled to a new trial as requested.

"A new trial is mandated where the error is not harmless beyond a reasonable doubt." ***Koch***, 39 A.3d at 1006. Harmless error exists where: (1) the error did not prejudice the defendant or the prejudice was de minimis; (2) the erroneously admitted evidence was merely cumulative of other untainted evidence which was substantially similar to the erroneously admitted

---

is not uncommon for a business to keep and rely upon the records of another business as a part of their own. In ***Bayview Loan Servicing LLC v. Wicker***, 206 A.3d 474 (Pa. 2019), our Supreme Court considered the business records exception in the context of the increasingly common situation where a loan is originated by one company but is later acquired by a separate company. The question was whether the records containing information originally recorded by the first company could be authenticated by an employee of the current holder of the loan or whether the litigant had to provide an employee of each of the prior holders of the loan or a certification of the records under Rule 902(11) or (12). Unlike the federal courts which have adopted a "rule of incorporation" which provides that the record a business takes custody of is "made" by the business, ***see, Commonwealth Financial Systems, Inc. v. Smith***, 15 A. 3d 492, 496 (Pa. Super. 2011), our Supreme Court has declined to adopt any bright line rule either forbidding the authentication of documents recorded by a third party or endorsing an automatic incorporation doctrine into the business records exception. Instead, it is the Court's position to continue to allow our trial courts to utilize their broad discretion in evidentiary matters by applying the business record exception of Rule 803(6) to determine if a witness "can provide sufficient information relating to the preparation and maintenance of the records to justify a presumption of trustworthiness" subject to the opponent rebutting the evidence with any other circumstances indicating a lack of trustworthiness. ***Bayview Loan***, 206 A.3d at 486.

evidence; or (3) the properly admitted and uncontradicted evidence of guilt was so overwhelming and the prejudicial effect of the error was so insignificant by comparison that the error could not have contributed to the verdict. ***Commonwealth v. Robinson***, 721 A.2d 344, 350 (Pa. 1999). Whenever there is a "reasonable possibility" that an error "could have contributed to the verdict," the error is not harmless. ***Commonwealth v. Passmore,*** 857 A.2d 697, 711 (Pa. Super. 2004).

As to Appellant's convictions on Counts 1-20 (possession of CSAM), we conclude that the admission of Exhibit 2 was not prejudicial error. This is because Corporal Brown, upon execution of his search warrant, searched Appellant's residence and found numerous electronic devices[23] belonging to Appellant.[24] After the items were seized, Corporal Brown examined the devices for CSAM. He testified that he found CSAM within the Samsung and

---

[23] ***See*** Commonwealth's Exhibit 1 – white cell phone case, tablet, black and red cell phone case, gray TCL Cricket phone, and Samsung Android phone.

[24] When asked by the trial court if Appellant was challenging the search warrant, Appellant replied only to the extent it was based on the illegally seized information in violation of the constitution. N.T. Suppression, 11/17/24, at 15. Appellant's argument makes clear the focus of his suppression motion was not upon any hearsay supporting the search warrant, but rather a claim that the ESPs and NCMEC were at all times acting as government agents and not as private actors. ***Id.*** at 5-6. In any event, it is settled that a warrant may be based upon hearsay, a different issue from the admissibility of evidence at trial. ***See Commonwealth v. Lyons,*** 79 A.3d 1053, 1064 (Pa. 2013) (probable cause supporting a search warrant may be based upon a totality of the circumstances set forth in the affidavit of probable cause, including the reliability and veracity of hearsay statements included therein).

TCL cell phones; however, he was only able to extract data from the Samsung phone. Images recovered from the Samsung phone were shown to the jury. This evidence was independent of Exhibit 2. With the electronic evidence in hand, the Commonwealth did not need to rely upon Exhibit 2 for the possession convictions.

We also observe from our examination of Exhibit 2 that the exhibit does not contain any images but merely identifies computer files which were flagged by an algorithm as containing CSAM. In comparison to the images shown to the jury from Appellant's devices, the electronic references found within Exhibit 2 would seem to carry much less weight than the actual images shown to the jury. In light of these considerations, we conclude that the improper admission of Exhibit 2 did not prejudice Appellant and/or the exhibit, at best, was cumulative of other untainted evidence with respect to Counts 1-20.

Likewise, we conclude that the admission of Exhibit 2 did not prejudice Appellant's conviction under Count 22 – criminal use of a communication facility. Appellant's use of his phone(s) to upload and/or to download CSAM was discovered by police after searching his cell phones. The conviction for this crime, at least for the underlying felony for possession, depended upon police finding CSAM on Appellant's electronic devices. The evidence of CSAM on Appellant's phones was sufficient to convict on this single count of the criminal use of a communication facility. Evidence to prove this offense was

not dependent on any evidence found within Exhibit 2. There was no prejudice that would warrant a new trial on Count 22.

The same cannot be said for the single conviction at Count 21 (dissemination). The improper admission of Exhibit 2 was the only evidence relied upon to support the conviction for dissemination of CSAM.[25] When asked during trial, Corporal Brown testified that the CyberTipline report in Exhibit 2 was the only evidence to support dissemination. N.T. Trial, 12/3/24, at 68. As no other evidence was presented to support a conviction on this count, the introduction of Exhibit 2 into evidence clearly caused prejudice to Appellant. This prejudice constitutes reversible error. Therefore, a new trial for Count 21 is warranted.

Accordingly, we affirm the convictions at Counts 1-20 and 22, reverse the conviction at Count 21, vacate the judgment of sentence, and remand for resentencing on Counts 1-20, and 22, and grant a new trial on Count 21.

Judgment of sentence vacated. Conviction at Count 21 reversed, remaining convictions affirmed. Remand for resentencing on Counts 1-20, and 22. A new trial is granted as to Count 21. Jurisdiction relinquished.

---

[25] Exhibit 2 was improperly admitted on the basis of hearsay where the Commonwealth attempted to use the exhibit to establish the truth of the information in that exhibit that Appellant distributed CSAM. While this exhibit *may* have been introduced to explain the course of the police investigation, admitting the exhibit on that basis could not be used as substantive evidence to prove the offense. ***See Commonwealth v. Palsa***, 555 A.2d 808 (Pa. 1989) (evidence admitted explaining the course of police conduct cannot be considered as substantive evidence of guilt).

Judgment Entered.

Benjamin D. Kohler

Benjamin D. Kohler, Esq.
Prothonotary

DATE: 9/21/2026