2023 PA Super 72

COMMONWEALTH OF PENNSYLVANIA : IN THE SUPERIOR COURT OF

PENNSYLVANIA

:

JOHN EDWARD KURTZ

٧.

.

Appellant : No. 811 MDA 2021

Appeal from the Judgment of Sentence Entered March 2, 2021 In the Court of Common Pleas of Northumberland County Criminal Division at No(s): CP-49-CR-0000045-2018

COMMONWEALTH OF PENNSYLVANIA : IN THE SUPERIOR COURT OF

PENNSYLVANIA

V.

Appellant

:

JOHN EDWARD KURTZ

No. 421 MDA 2023

Appeal from the Judgment of Sentence Entered March 2, 2021 In the Court of Common Pleas of Northumberland County Criminal Division at No(s): CP-49-CR-0001236-2018

COMMONWEALTH OF PENNSYLVANIA : IN THE SUPERIOR COURT OF

PENNSYLVANIA

٧.

:

JOHN EDWARD KURTZ

:

Appellant : No. 429 MDA 2023

Appeal from the Judgment of Sentence Entered March 2, 2021 In the Court of Common Pleas of Northumberland County Criminal Division at No(s): CP-49-CR-0001479-2018

BEFORE: MURRAY, J., McLAUGHLIN, J., and COLINS, J.*

OPINION BY COLINS, J.:

FILED: APRIL 28, 2023

Appellant, John Edward Kurtz, appeals from the judgment of sentence imposed following his conviction of numerous offenses, including rape, kidnapping, attempted rape, and attempted kidnapping, involving five victims. After careful review, we affirm.

On the evening of July 19, 2016, K.M. went to sleep in her home in Northumberland County after her husband left for his overnight shift at a correctional facility. When K.M. was awakened by her barking dogs and left her bedroom to investigate, a man jumped out of one of her empty bedrooms, tied her hands behind her back with zip ties, blindfolded her, placed a gag in her mouth, and struck her several times. The man then dragged K.M. outside and into his vehicle and transported her to a camper, where he vaginally and anally raped her. After being released in a corn field close to her home, K.M. found her way to a residence and the Pennsylvania State Police ("PSP") were called. K.M. was taken to a hospital where sperm was collected from her anus; DNA was ultimately extracted from the sperm.

On September 14, 2016, PSP obtained a search warrant directed to Google, Inc. for records of searches made with Google's search engine for K.M.'s name or home address during the week preceding the July 2016 incident. On November 29, 2017, Google returned a report that identified an

* Retired Senior Judge assigned to the Superior Court.

internet protocol ("IP") address as having conducted two searches of K.M.'s address several hours before the attack. PSP later determined through requests submitted to the American Registry of Internet Numbers and Appellant's telecommunications service provider that the IP address corresponded to Appellant.

PSP began to conduct 24-hour surveillance of Appellant, who troopers soon discovered was employed as a corrections officer at the same facility as K.M.'s husband. During the course of the surveillance, troopers retrieved a cigarette butt that Appellant discarded in a store parking lot.¹ DNA was extracted from the cigarette butt, which was determined to match the DNA collected from K.M.

PSP arrested Appellant on December 18, 2017. During the course of a police interview, Appellant admitted to having committed the kidnapping and rape of K.M. In addition, Appellant incriminated himself in four other incidents involving victims D.S., H.Z., A.H., and T.S. Appellant also led the investigating troopers to the residences of D.S., A.H., and T.S.

D.S. testified at trial that she was alone in her home on the morning of November 9, 2012, after just having seen her husband off to work, when she discovered a masked man in her home. The man ordered her to lay down on her stomach on the floor, zip tied her hands, restrained her legs, blindfolded

- 3 -

¹ K.M., as well as other victims, testified that they recalled their assailant to be smoking during their encounters.

her, and placed a gag in her mouth. The man then wrapped D.S. in a sheet and carried her to the basement. After D.S. pleaded with her attacker for some time, he cut the zip ties and left without sexually assaulting her. DNA was collected from the crime scene and later determined to match Appellant.

H.Z. testified that late in the evening on April 22, 2017 or in the early morning of the following day, she awoke in her home to discover a man on top of her zip tying her hands behind her back. The man blindfolded her and gagged her, wrapped a sheet around her, and carried her to a vehicle. H.Z. was transported to another residence where she was secured to a bed and vaginally raped. A DNA sample collected from H.Z. was found to match Appellant.

A.H. testified that on several occasions in 2015, she discovered signs that someone had entered the home that she shared with her two young children. A.H. described finding doors to the outside having been inexplicably left open, hearing a male voice coming from her basement in the middle of the night, and hearing footsteps and doors slamming inside her house.

Finally, T.S. testified that, on June 3, 2015, she was sleeping at her home in Columbia County when she was awoken by a man who had placed his hand over her mouth and instructed her not to scream or he would hurt her children sleeping in the next room. The intruder zip tied her hands behind her back and blindfolded her. According to T.S., the man then said "he didn't know why he was doing this," got off T.S.'s back, and cut off the zip ties. N.T. (Trial), at 306. The intruder left without sexually assaulting her.

Appellant was charged at three separate dockets with offenses related to the five victims.² The Commonwealth filed a motion to consolidate the three matters, while Appellant filed a motion to sever. On January 18, 2019, the trial court granted the motion to consolidate the cases and denied the motion to sever.

Appellant filed an omnibus pre-trial motion, in which he sought the suppression of the evidence that Google searches of K.M.'s residence were conducted from his IP address in the hours prior to the attack. In addition, through a motion *in limine*, Appellant sought to suppress the Google evidence based upon the Commonwealth's mishandling of the electronic file provided by Google, which Appellant alleged prevented him from being able to verify that the file had not been manipulated. After holding hearings, the trial court denied these motions by orders entered July 23, 2018 and August 18, 2020.

-

² Appellant was charged at CP-49-CR-0000045-2018 with offenses relating to victims K.M., D.S., and H.Z., which occurred in Northumberland County. The charges relating to victims A.H. and T.S. were initially filed in Montour County and Columbia County, respectively, where those incidents occurred; following the transfer of those cases to Northumberland County in 2018, they were given the trial court docket numbers of CP-49-CR-0001236-2018 and CP-49-CR-0001479-2018, respectively.

Appellant further requested in his motion *in limine*³ that the trial court suppress "tower dump" evidence⁴ obtained from AT&T, which showed all of the cellular devices connected to the AT&T antenna that serviced the area of T.S.'s residence during the approximate five-hour range of time that the intruder was inside her home on June 3, 2015. Appellant objected because PSP requested these records using a court order under Section 5743 of the Wiretapping and Electronic Surveillance Control Act ("Wiretap Act"), 18 Pa.C.S. § 5743, rather than a warrant supported by probable cause and individualized suspicion that Appellant was engaged in criminal activity. The trial court denied suppression in its August 18, 2020 order.

Appellant's jury trial began on October 5, 2020. On October 14, 2020, the jury returned a verdict of guilty on all counts.⁵ On March 2, 2021, the trial

_

³ While Appellant raised the issues related to the tower dump and the Commonwealth's mishandling of the Google file in a motion *in limine* filed on April 14, 2020, the relief he sought would be more properly characterized as the suppression of this evidence. However, as this Court has explained, for the purposes of an appeal, a trial court's ruling on a motion *in limine* has the same practical effect as a ruling on a pre-trial suppression motion. **See Commonwealth v. Padilla**, 923 A.2d 1189, 1194 (Pa. Super. 2007).

⁴ A "tower dump" is "a download of information on all the devices that connected to a particular cell site during a particular interval." *Carpenter v. United States*, 138 S.Ct. 2206, 2220 (2018).

⁵ Appellant was convicted of multiple counts each of rape, kidnapping, attempted rape, attempted kidnapping, aggravated assault, burglary, involuntary deviate sexual intercourse, sexual assault, simple assault, unlawful restraint, false imprisonment, and loitering and prowling at nighttime, as well as and a single count of strangulation. 18 Pa.C.S. §§ 901(a), 2701(a)(1), 2702(a)(1), 2902(a)(1), 2903(a), 2718(a)(2), 2901(a)(2), (3), 3121(a)(1), (2), 3123(a)(1), 3124.1, 3502(a)(1), 5506.

court sentenced Appellant to an aggregate term of imprisonment of 59 to 280 years. Appellant filed a timely post-sentence motion, which the trial court denied by opinion and order entered on May 17, 2021. Appellant then filed this timely appeal.⁶ Appellant and the trial court have complied with Pa.R.A.P. 1925.

Appellant raises the following issues on appeal:

- A. Whether the trial court erred in allowing the admission of unauthenticated, illegally obtained evidence because the investigatory search warrant lacked probable cause?
- B. Whether the trial court erred by allowing the admission of cell tower evidence that was the product of an invalid search warrant?
- C. Whether the trial court erred by failing to sever three separate cases, which severely prejudiced the outcome of the case and stripped the Appellant of his due process rights?
- D. Whether the trial court erred by imposing an excessive sentence upon the Appellant by failing to take several variables into consideration?

Appellant's Brief at 4 (unnecessary capitalization and suggested answers omitted).

March 6, 2023 directing Appellant to file amended notices of appeal at each trial court docket to correct the procedural error. Appellant has complied with our directive.

⁶ Appellant initially filed a single notice of appeal listing all three trial court docket numbers in violation of *Commonwealth v. Walker*, 185 A.3d 969 (Pa. 2018), and Pa.R.A.P. 341. In accordance with our Supreme Court's decision in *Commonwealth v. Young*, 265 A.3d 462 (Pa. 2021), and pursuant to our authority under Pa.R.A.P. 902, this Court entered an order on

Google Search

In his first issue, Appellant objects to the admission of the evidence showing two Google searches of K.M.'s residence from his IP address⁷ hours prior to her kidnapping and rape. This argument proceeds in several parts, but we first address Appellant's argument that the trial court erroneously denied suppression of the search warrant served upon Google. Appellant contends that the affidavit of probable cause in support of the warrant was merely speculative and did not set forth grounds that an individual of reasonable caution would believe that the perpetrator of the assault of K.M. used the Google search engine when planning the crimes. Appellant asserts that he had a reasonable expectation of privacy over his Google search queries, as it is nearly impossible to participate in contemporary society without conducting internet searches. In addition, Appellant argues that he did not lose his privacy interest in his searches as a result of his assent to Google's privacy policy, which only authorized search results to be turned over in response to legally enforceable requests.

Our standard of review of a trial court's ruling on a suppression motion is "whether the factual findings are supported by the record and whether the legal conclusions drawn from those facts are correct." *Commonwealth v. Rosario*, 248 A.3d 599, 607 (Pa. Super. 2021) (citation omitted). We are

 $^{^7}$ An IP address is an identifying number assigned by an internet service provider to an individual user that facilitates the transfer of data across the internet. N.T., 5/22/18, at 7-8.

bound by the facts found by the trial court so long as they are supported by the record, but we review its legal conclusions *de novo*. *Id.* at 607-08. The trial court has sole authority to pass on the credibility of witnesses and the weight to be given to their testimony. *Id.* at 608. "Our scope of review is limited to the record developed at the suppression hearing, considering the evidence presented by the Commonwealth as the prevailing party and any uncontradicted evidence presented by the defendant." *Commonwealth v. Kane*, 210 A.3d 324, 329 (Pa. Super. 2019) (citation and brackets omitted).

Here, the trial court rejected Appellant's argument that the search warrant directed to Google was not supported by probable cause, finding that there was a fair probability based upon the information in the possession of law enforcement that the individual who attacked K.M. stalked her online by searching for her address. Order, 7/23/18, ¶3. In addition, the court found that Appellant lacked a reasonable expectation of privacy in his IP address as well as the search queries he entered into the Google search engine. *Id.*, ¶¶1-2. We agree with the trial court's determination that the Google warrant was supported by probable cause and that Appellant lacked a reasonable expectation of privacy, and therefore we affirm the denial of the suppression motion on both grounds.

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." *Kane*, 210 A.3d at 330. In determining whether the defendant'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." *Id.* (citation and quotation marks omitted). "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." *Id.* (citation omitted).

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. **Id.** 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. **Commonwealth v. Duncan**,

817 A.2d 455, 462-63 (Pa. 2003); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1290-91 (Pa. 1979).⁸

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. *Id.* 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, 830-31 (Pa. Super. 2001) (citation omitted), *affirmed*, 837 A.2d 1163 (Pa. 2003). We have likewise

⁸ In **DeJohn**, the Court initially rejected **Miller** outright as applied to warrantless requests for bank records, but the Court in **Duncan** limited the broader protection under the Pennsylvania Constitution to substantive bank records. In **Duncan**, officers investigating a rape obtained surveillance video from a shop showing an individual matching the description of the assailant attempting to make a purchase with an ATM card, but his card was rejected. 817 A.2d at 457. The officers then called the manager of the issuing bank and obtained the name and address of the holder of the identified account. **Id.** The Court distinguished this request as distinct from one that would reveal the substantive details of the customer's financial affairs, noting that officers "were looking for the mere **identity** of the person they had strong reason to believe had forcibly raped a woman, and who had attempted to use a precisely identified ATM card." **Id.** at 462 (emphasis in original).

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); *see 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).

At the suppression hearing in this case, the Commonwealth introduced Google's privacy policy that was in effect in July 2016 when the relevant searches were performed. N.T., 5/22/18, Commonwealth Exhibit 4 (Google Privacy Policy, last modified 6/28/16). The privacy policy details the information that Google collects and when it will share that information outside of the company:

We collect information about the services that you use and how you use them . . .

We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number) . . .

When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes . . . details of how you used our service, such as your search queries[,] . . . [and IP] address . . .

We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to . . . meet any applicable law, regulation, legal process or enforceable governmental request.

Id. at 1-2, 4 (emphasis omitted; some reformatting). By accessing Google's search engine, users agree to be bound by Google's terms of service. N.T., 5/22/18, at 11.

We conclude that Appellant lacked a reasonable expectation of privacy concerning his Google searches of K.M.'s home address and his IP address. By typing in his search query into the search engine and pressing enter, Appellant affirmatively turned over the contents of his search to Google, a third party, and voluntarily relinquished his privacy interest in the search. **Sodomsky**, 939 A.2d at 369; **Proetto**, 771 A.2d at 830-31. The fact that Appellant lost his reasonable expectation of privacy over his search query is reinforced by Google's privacy policy, which specifically allowed for the company to turn over search results when requested by law enforcement and

which he assented to by using the company's search service. Dunkins II, 263 A.3d at 255-56. Furthermore, Appellant lacked a reasonable privacy interest in his IP address because the IP address served as the manner in which Google's servers communicated with his computer. Christie, 624 F.3d at 573-74; Duncan, 817 A.2d at 462-63.

In arguing that he had a reasonable expectation of privacy over the searches of K.M.'s address, Appellant refers us to the United States Supreme Court's decision in *Carpenter v. United States*, 138 S.Ct. 2206 (2018), which 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, or cell site. *Id.* at 2211-12. 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"

_

⁹ While Appellant argues that the Google privacy policy is irrelevant to our analysis because the policy is a "contract of adhesion," Appellant's Brief at 41, the question before us is not whether Appellant is bound by the terms of the agreement under traditional contract interpretation principles but whether he was aware that his search queries could be turned over to a third party thus vitiating the reasonableness of his privacy expectation. We find that the privacy policy clearly communicated that Google may share its users' search queries, including in response to law enforcement requests.

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.* (citation and quotation marks omitted).

Appellant's searches are distinct from the CSLI at issue in *Carpenter* because the Google evidence was not passively collected, but instead Appellant affirmatively chose to type in K.M.'s address and submit the search request notwithstanding the company's privacy policy providing that it collects and shares search queries. Furthermore, unlike *Carpenter*, the information provided by Google here did not offer anything like a "detailed chronicle" of Appellant's movements. Id. Rather, the Google warrant was limited in nature, requesting only information on searches over a discrete seven-day period for the name of one person or one physical address associated with a violent felony. Google was not authorized to create a log of all of Appellant's search queries or the websites he visited, and the warrant did not require production of data that shed light on Appellant's political views, health information, or other sensitive matters. We therefore find Carpenter inapposite as to the application of the third-party doctrine concerning the Google search warrant.¹⁰

¹⁰ We further observe that the Court's decision in *Carpenter* that the third-party doctrine does not apply to CSLI has not affected the unanimity in the federal courts that IP addresses lack Fourth Amendment privacy protection. *See Trader*, 981 F.3d at 967-68; *Morel*, 922 F.3d at 9.

Even if Appellant did have a constitutionally cognizable privacy interest in his searches of K.M.'s address, we would also find that the Google warrant was supported by probable cause. "The Fourth Amendment to the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution guarantee the right of the people to be secure in their persons, houses, papers, and possessions from unreasonable searches and seizures." Commonwealth v. Thomas, 273 A.3d 1190, 1195 (Pa. Super. 2022). Article I, Section 8 and the Fourth Amendment each require that, prior to conducting a search, law enforcement must obtain a warrant supported by probable cause and issued by a neutral magistrate. Commonwealth v. Glass, 200 A.3d 477, 488 (Pa. Super. 2018). "Probable cause exists where the facts and circumstances within the affiant's knowledge and of which he has reasonably trustworthy information are sufficient in themselves to warrant [an individual] of reasonable caution in the belief that a search should be conducted." **Pacheco**, 263 A.3d at 645 (citation omitted).

The task of the issuing authority in approving a warrant is to "to make a practical, common[-]sense assessment of whether, given all the circumstances set forth in the affidavit, a fair probability exists that contraband or evidence of a crime will be found in a particular place." **Commonwealth v. Harlan**, 208 A.3d 497, 505 (Pa. Super. 2019) (citation omitted). "The reviewing court is not to conduct a *de novo* review of the issuing authority's probable cause determination[] but is simply to determine whether or not there is substantial evidence in the record supporting the

decision to issue a warrant." *Commonwealth v. Mendoza*, 287 A.3d 457, 463 (Pa. Super. 2022) (citation omitted). "In so doing, the reviewing court must accord deference to the issuing authority's probable cause determination[] and must view the information offered to establish probable cause in a common-sense, non-technical manner." *Id.* (citation omitted).

Here, the affidavit of probable cause in support of the search warrant application explained that an attacker confronted K.M. in her home at approximately 1:45 a.m. on July 20, 2016, and then gagged, blindfolded, restrained with zip ties, and choked her to unconsciousness, before moving her to another location by vehicle. N.T., 5/22/18, Commonwealth Exhibit 6 (Search Warrant Application, 9/14/16). After the sexual assault, K.M.'s assailant left her in a cornfield .7 miles from her home. *Id.*

The affiant, Trooper Joel Follmer, stated that, based upon the nature of the assault, there was a reasonable probability that K.M.'s attacker had researched her name or her address prior to the date of the incident. *Id.* This conclusion was based upon the remote nature of K.M.'s residence, which was not visible to most passersby, indicating that K.M. was not randomly targeted; instead, the perpetrator was familiar with K.M. and her residence, possibly after seeing her in the community and then planning the crime. *Id.* Furthermore, because many sexual offenders are predominantly fantasy driven, there was a basis to conclude that K.M.'s assailant may have been stalking her over a period of time. *Id.* In addition, K.M. was attacked at a time when her husband was at work on an overnight shift, an indication that

the actor may have spent time tracking her and researching her husband's work schedule. *Id.* Due to the widespread availability of Google's search engine, Trooper Follmer thus sought to compel Google to turn over the IP addresses for users who conducted searches for K.M.'s name or home address in the seven days prior to her attack. *Id.*

We agree with the trial court that the search warrant set forth grounds to show a "fair probability" that the Google search information would uncover evidence related to K.M.'s sexual assault, specifically the identity of her attacker. *Harlan*, 208 A.3d at 505 (citation omitted). The circumstances set forth in the search warrant—namely the secluded location of the residence, the drop-off location close to K.M.'s home but also in an isolated area, the fact that the attack happened at a time when K.M. was asleep at home and her husband was working, and the potential fantasy driven motivation for the perpetrators of this type of sexual assault—showed reasonable grounds to conclude that the sexual assault was not random or spur of the moment. Rather, a "practical, common sense assessment" of these factors reasonably led the investigating officers, as well as the issuing magistrate, to conclude that the assault of K.M. was conducted after significant planning, and that planning was particularly focused on the situs where the events occurred. **Id.** (citation omitted). Furthermore, it was reasonable to conclude, due to the ubiquity of internet search engines and Google's services in particular, that the planning of the crime would take advantage of Google's search engine.

Moreover, we are unpersuaded by Appellant's claims that the affidavit was improperly based upon "general assumptions rather than specific and articulable facts" and that it lacked "concrete evidence" that the perpetrator of K.M.'s assault used Google. Appellant's Brief at 19. The search warrant did not simply assert that a crime occurred at a certain place and ask for all Google searches related to that location. Instead, Trooper Follmer articulated various circumstances he discovered during his investigation indicating that the crime was well-planned, including the secluded locations of K.M.'s house and the field where K.M. was dropped off, the timing of the crime when K.M.'s husband was at work, and the typical profile of perpetrators of this type of sexual assaults. Furthermore, Appellant's contention that the warrant needed to lay out "concrete evidence" that Appellant had used Google's services, id., is in conflict with the probable cause standard, which requires only that there is a "fair probability" that the search will be fruitful. *Harlan*, 208 A.3d at 505 Granting the appropriate deference to the issuing (citation omitted). authority's probable cause determination, we see no error in the trial court's conclusion that the facts alleged in the warrant were sufficient to warrant an individual of reasonable caution to believe that a search should be conducted.

Pacheco, 263 A.3d at 645.¹¹

-

¹¹ Appellant argues that other evidence offered against him—including DNA evidence and his confessions to the investigating officers—were fruit of the poisonous tree as the additional evidence was obtained as a result of information discovered pursuant to the allegedly unlawful Google search (Footnote Continued Next Page)

Appellant further argues that the trial court should have suppressed the evidence Google produced in response to the search warrant because the PSP inadvertently deleted "hash value" metadata information associated with the electronic file that Google provided when they saved the file in Microsoft Excel's XLSX file format instead of its original CSV format. Appellant asserts that the Google evidence was "extremely relevant" to this case and the "integrity and certification of this information was and still is paramount." Appellant's Brief at 37. Appellant contends that PSP was neglectful of its "duty to maintain the integrity and authenticity of the evidence that they acquire" and he was "subjected to extreme prejudice" by the admission of the unverified Google information. *Id.* at 37-38.

Appellant's argument implicates his due process rights to access evidence under the United States Constitution. In *Commonwealth v. Snyder*, 963 A.2d 396 (Pa. 2009), our Supreme Court held that, when the government loses or destroys evidence, the trial court must determine

warrant. However, because we have found that there was no "antecedent illegality" with respect to the Google warrant, the fruit of the poisonous tree doctrine has no application here. *Commonwealth v. Torres*, 177 A.3d 263,

Appellant also argues over the course of a few sentences in his brief that his confessions to the investigating officers should have been suppressed because he was coerced into waiving his right to counsel. Appellant's Brief at 42. This argument, however, is devoid of any citations to the record or applicable caselaw. Nor does Appellant offer any specificity on the manner in which PSP supposedly coerced him into confessing. As Appellant has failed to develop this argument in any meaningful fashion, we find it waived. **Wirth v.**

Commonwealth, 95 A.3d 822, 837 (Pa. 2014).

276 (Pa. Super. 2017) (citation omitted).

whether the unavailable evidence is "potentially useful" or "materially exculpatory"; if it is only potentially useful, then the defendant must show bad faith by the Commonwealth to have the evidence suppressed. *Id.* at 403-06. Our Supreme Court has further explained:

[T]he Due Process Clause [] requires defendants be provided access to certain kinds of evidence prior to trial, so they may be afforded a meaningful opportunity to present a complete defense. This guarantee of access to evidence requires the prosecution to turn over, if requested, any evidence which is exculpatory and material to guilt or punishment, **see** [**Brady v. Maryland**, 373 U.S. 83 (1963)], and to turn over exculpatory evidence which might raise a reasonable doubt about a defendant's guilt, even if the defense fails to request it, **see United States v. Agurs**, 427 U.S. 97[] (1976). If a defendant asserts a **Brady** or **Agurs** violation, he is not required to show bad faith.

There is another category of constitutionally guaranteed access to evidence, which involves evidence that is not materially exculpatory, but is potentially useful, that is destroyed by the state before the defense has an opportunity to examine it. When the state fails to preserve evidence that is "potentially useful," there is no federal due process violation unless a criminal defendant can show bad faith on the part of the police. Potentially useful evidence is that of which no more can be said than that it could have been subjected to tests, the results of which might have exonerated the defendant. In evaluating a claim that the Commonwealth's failure to preserve evidence violated a criminal defendant's federal due process rights, a court must first determine whether the missing evidence is materially exculpatory or potentially useful.

Commonwealth v. Chamberlain, 30 A.3d 381, 402 (Pa. 2011) (some citations and quotation marks omitted).

Following a hearing, the trial court denied suppression of the Google search results in its August 18, 2020 order, ruling as follows:

- 1. The [PSP] testimony was credible as to how the file was converted from a [CSV] file to an [XLSX] file; it was simply that the file was saved under the wrong format by a Trooper that had opened the [CSV] as given and by saving it, converted it to the [XLSX]. Google provided a certificate of authenticity to the Commonwealth which was in turn provided to [Appellant].
- 2. The [CSV] file sought to be examined by [Appellant's] experts is only "potentially useful" rather than "materially exculpatory" evidence; thus, the file is only subject to suppression if the Commonwealth acted in bad faith; and here, it did not.
- 3. None of the facts presented give rise to the notion that this [CSV] file was converted in bad faith by [PSP].

Order, 8/18/20, $\P\P1-3$ (footnotes omitted).

Upon review, we discern no error in its analysis. The testimony at the hearing established that a hash value is a mathematical equation associated with the data in an electronic file that acts as a forensic "fingerprint[]" on the file. N.T., 7/9/20, at 8-9, 32. Trooper Follmer testified that he accessed the CSV-format file produced in response to the search warrant from Google's law enforcement portal, opened the spreadsheet in Microsoft Excel, and then saved it as an XLSX file. *Id.* at 24-25. After discovering that his act of saving the file in a different format deleted the original hash value, he attempted to log back into the back into the Google portal, but the CSV file was gone; he also contacted Google and looked through various PSP computers to find the original file, but his efforts were fruitless. *Id.* at 26-27. Trooper Follmer stated that he made no alterations to the spreadsheet produced by Google, and he had no training in computer forensics such that he was aware that he would delete the hash value when he saved the file in Excel format. *Id.* at

25. The Commonwealth's computer forensics expert confirmed that the act of saving the CSV file in XLSX format was sufficient to destroy the original hash value, that PSP computers prompted users to save spreadsheets in Microsoft's proprietary format, and the fact that the hash value was unrecoverable was not a sign of manipulation of the search results. *Id.* at 33, 36, 39-41.

The record thus supports the trial court's conclusion that the hash value was only potentially useful to Appellant and not materially exculpatory. While Appellant's computer forensics expert testified that he was unable to determine the authenticity of the file produced by PSP because he could not trace the hash value back to Google, id. at 8-13, he did not show that PSP had actually tampered with the file. An allegation that missing evidence, if subject to additional testing, may have proven to be exculpatory does not turn "potentially useful" evidence into "materially exculpatory" evidence. See Snyder, 963 A.2d at 406 (soil samples that showed presence of toxins in government testing before being destroyed were not materially exculpatory where defendant merely speculated that independent testing would show different results); Commonwealth v. Ward, 188 A.3d 1301, 1309 (Pa. Super. 2018) (vehicle where shooting occurred that was not preserved by government was not "materially exculpatory" based upon defendant's conjecture that "if his expert had been able to examine the car, he might have found evidence that" would have supported self-defense claim) (emphasis in original).

As Appellant's allegation of any exculpatory value to the hash value was speculative, he was required to prove that the Commonwealth acted in bad faith in allowing the hash value to be destroyed before suppression would be ordered. **See Chamberlain**, 30 A.3d at 402-03; **Snyder**, 963 A.2d at 406. However, as the trial court noted, no evidence was presented that the Commonwealth acted in bad faith in destroying the original hash value as it was simply the result of Trooper Follmer opening a CSV file in Microsoft Excel and then saving it in the prompted format. As the trial court's finding of an absence of bad faith is supported by the record, this determination is conclusive on appeal. **See Chamberlain**, 30 A.3d at 402 ("Because the trial court's factual findings [that the Commonwealth did not act in bad faith in its handling of evidence that it allowed to be destroyed] are supported by the record, we must defer to them."). Therefore, because the hash value was only potentially useful and PSP did not act in bad faith in failing to preserve it, we affirm the trial court's denial of suppression.

Appellant next argues that his right to confrontation under the Sixth Amendment of the United States Constitution was violated when the Commonwealth admitted the spreadsheet showing the Google searches without presenting an employee of that company as a witness to authenticate the search results. Appellant contends that he "was unable to cross-examine the contents of the evidence generated by [] Google [] and was subject to severe prejudice" because the Google evidence was vital to the Commonwealth's case. Appellant's Brief at 39.

We conclude that Appellant has waived his Confrontation Clause challenge because he did not raise an objection on that basis at trial. Where a party claims error in the admission of evidence, the party must object and state the specific grounds for objection. Pa.R.E. 103(a)(1); *Commonwealth v. Wroten*, 257 A.3d 734, 742 (Pa. Super. 2021). The judge hearing the case must be given an opportunity to correct the error at the time it is made and potentially avoid an unnecessary appeal. *Commonwealth v. Rosser*, 135 A.3d 1077, 1086 (Pa. Super. 2016) (*en banc*). Furthermore, "[w]here the trial court denies relief on one theory, a defendant may not attain appellate relief on a new theory for that same relief." *Id.*

At trial, Appellant objected to the admission of the Google evidence for a variety of reasons but none of them were on the basis that his confrontation clause rights were violated.¹² Therefore, this issue was waived. **See id.** at

¹² **See** N.T. (Trial), at 428-41 (objecting to admission of Google spreadsheet on basis of lack of personal knowledge, hearsay, lack of authentication, lack of foundation, improper opinion testimony, and violation of best evidence rule).

To the extent Appellant's argument could be construed as a claim that the Google evidence was not properly authenticated, we find that claim to be devoid of merit. Authentication generally entails a relatively low burden of proof and requires only, as stated in Rule of Evidence 901, that the proponent "produce evidence sufficient to support a finding that the item is what the proponent claims it is." Pa.R.E. 901(a); *Commonwealth v. Jackson*, 283 A.3d 814, 818 (Pa. Super. 2022). Rule 901 can be satisfied with testimony of a witness with personal knowledge or by circumstantial evidence. *Jackson*, 283 A.3d at 818 (citing Pa.R.E. 901(b)(1), (4)).

At trial, Trooper Follmer testified regarding his preparation and submission of the Google search warrant through Google's online portal and then (Footnote Continued Next Page)

1087 (where defendant did not raise a Confrontation Clause claim in the trial court, the argument was waived on appeal); *Commonwealth v. Akbar*, 91 A.3d 227, 235 (Pa. Super. 2014), *vacated on other grounds*, 111 A.3d 168 (Pa. 2015) (Confrontation Clause issue waived where defendant only raised a hearsay objection at trial when evidence admitted).

Accordingly, we find no merit to each of Appellant's arguments challenging the denial of suppression of the Google evidence, as well as its admission at trial. Appellant is entitled to no relief on his first appellate issue.

Tower Dump

In his second appellate issue, Appellant argues that the trial court erred by refusing to suppress the evidence gathered through a "tower dump" request to AT&T related to his cell phone's access of the antenna servicing victim T.S.'s house during the hours when she was attacked. Appellant asserts that the legal process for obtaining the cell tower data, under Section 5743 of

downloading Google's spreadsheet in electronic format through the same portal. N.T. (Trial), at 173-74, 181-85, 427-28, 432-33, 437-40. Trooper Follmer explained that the spreadsheet was identified by the case name and contained other information connecting it to the K.M. investigation. *Id.* at 433, 437-40. Trooper Follmer's testimony that he downloaded the Google spreadsheet through the same portal in which he submitted the warrant, as well as circumstantial evidence that connected the document to K.M.'s case, was sufficient to meet the Commonwealth's burden to authenticate the Google spreadsheet. Pa.R.E. 901(b)(1), (4); *Jackson*, 283 A.3d at 818.

¹² Section 5743 provides that an order for disclosure shall be issued upon a showing by law enforcement of "specific and articulable facts" that "there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 Pa.C.S. § 5743(d).

the Wiretap Act, was not based upon probable cause and lacked any specificity as to the individual involved, the place to be searched, or what items were to be seized.¹³ Appellant contends that the seizure here implicated the same privacy interest at issue in *Carpenter* and *Pacheco*, relating to the records of an individual's movements captured through the collection of CSLI from telecommunications providers.

As explained at the hearing on Appellant's motion *in limine*, when law enforcement requests a tower dump, it identifies a specific location and specific time period, and the service provider determines "what cell towers would reasonably service" the location and compiles a record that "show[s] all of the subscribers that initiated communications across those towers in that area for the time span covered." N.T., 7/9/20, at 52. The information that is produced in a tower dump is automatically generated and routinely collected by the service provider. *Id.* Furthermore, unlike CSLI, a tower dump does not allow for the tracking of the movement of any individual cell-phone user but simply indicates all of the usage in a particular location during a particular time period. *Id.* at 28, 52.

In this matter, PSP obtained an order pursuant to the Wiretap Act requiring that AT&T provide a record of its subscribers whose phones accessed

_

¹³ Section 5743 provides that an order for disclosure shall be issued upon a showing by law enforcement of "specific and articulable facts" that "there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 Pa.C.S. § 5743(d).

the cell phone tower servicing the vicinity of T.S.'s home in a rural portion of Columbia County between 2:00 a.m. and 7:00 a.m. on June 3, 2015, the window of time in which the intruder was present inside her home. N.T. (Trial), at 530-34, 537, 543-52. AT&T produced a file showing over 40,000 incidences of cell-phone call, text, and data activity during this five-hour period, including 10 "hits" for Appellant's cell phone. *Id.* at 548-51, 558, 560, 567-68. The cell-phone tower at issue here provided service in a range of up to seven and a half miles. *Id.* at 566.

Carpenter concerned the government's warrantless collection of a fourmonth period of the defendant's CSLI, showing 13,000 connections by his cell phone to the closest radio antennas, or cell sites; the government was thus able to create "a comprehensive dossier of his physical movements" during a period in which nine Radio Shack and T-Mobile stores were robbed in Michigan and Ohio. Id. at 2211-13, 2220. After determining that individuals maintain a reasonable expectation of privacy in their CSLI, id. at 2216-20, the Court held that "the acquisition of the cell-site records [is] a search within the meaning of the Fourth Amendment" and that the government "must generally obtain a warrant supported by probable cause before acquiring such records."

Notably, the Court in *Carpenter* emphasized that its decision was "a narrow one" and it did "not express a view on matters not before" it, including real-time collection of CSLI and "tower dumps." *Id.* at 2220. The Supreme Court further stated that its decision was not calling in to question

"conventional surveillance techniques and tools, such as security cameras . . . or business records that might incidentally reveal location information." *Id.*

In *Pacheco*, our Supreme Court extended the reasoning of *Carpenter* to real-time CSLI, concluding that "*Carpenter*'s warrant requirement for the collection of historical CSLI . . . applies with equal force to the collection of real-time CSLI." 263 A.3d at 640. The Court did not address tower dumps in its decision except to note that *Carpenter* specifically excluded that type of search from its Fourth Amendment analysis. *Id.* at 639 n.13.

Thus, neither *Carpenter* nor *Pacheco* squarely address tower dumps. This Court considered an analogous search, however, in *Commonwealth v. Dunkins*, 229 A.3d 622 (Pa. Super. 2020) ("*Dunkins II*"), *affirmed*, *Dunkins II*, 263 A.3d 247 (Pa. 2021). In that case, two men entered a college dormitory and pretended to be campus police in an effort to obtain access to one of the dorm rooms; once inside the dorm room, they assaulted and robbed the occupants. *Id.* at 625. While investigating the incident, campus police obtained a list of the students logged on to the wireless ("WiFi") network access point in the dorm, which ultimately led them to conclude that Dunkins was one of the individuals who had perpetrated the attack. *Id.*

On appeal, Dunkins challenged the denial of his suppression motion regarding the wireless network evidence, relying principally on *Carpenter*. However, this Court noted that the *Carpenter* ruling was narrowly confined to the context of historical CSLI searches and did not address other related types of searches, including tower dumps. *Id.* at 629. We stated that the

campus police's actions were "akin to a 'tower dump' request" from the college's IT department for "general network connection" data for the wireless access point closest to the robbery. *Id.* As we noted, the "campus police did not target a specific individual or attempt to track an individual's movements but instead merely sought to compile a list of all the devices signed on to the WiFi in the [] dorm at the time of the robbery." *Id.* We distinguished the collection of data in *Dunkins* from the CSLI obtained in *Carpenter*, noting that the CSLI allowed the police to track an individual's movements at all times of the day, while the WiFi data only showed access at one location at a particular time. *Id.* We thus found no error in the trial court's denial of the suppression motion challenge to the warrantless search of the WiFi data. *Id.*¹⁴

Furthermore, following *Carpenter*, various federal courts have declined to extend the Supreme Court's ruling to tower dump searches. For example, in *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019) (*per curiam*), the Seventh Circuit Court of Appeals concluded that the appellant's privacy interests were not infringed based upon the government's collection of tower dump data from antennas that serviced the area of two cell-phone stores where robberies occurred. *Id.* at 610-11. The court of appeals explained that

_

¹⁴ We stated as alternate grounds for affirmance the fact that the defendant had voluntarily consented to the college's computing resources policy, which clearly stated that users had no right to privacy over their use of the WiFi network. **Dunkins I**, 229 A.3d at 630-31. As noted above, our Supreme Court affirmed our decision in **Dunkins I**, relying on the alternate grounds that the defendant abandoned his right to privacy by assenting to the computing resources policy. **Dunkins II**, 263 A.3d at 255-56.

"Carpenter itself does not help" the appellant, as that "case did not invalidate warrantless tower dumps (which identified phones near one location (the victim stores) at one time (during the robberies)) because the Supreme Court declined to rule that these dumps were searches requiring warrants." *Id.* at 611 (emphasis in original); *accord United States v. Rhodes*, 2021 WL 1541050, at *1-2 (N.D. Ga. filed Apr. 20, 2021); *United States v. Walker*, 2020 WL 4065980, at *7-8 (E.D.N.C. filed July 20, 2020), *affirmed on other grounds*, 32 F.4th 377 (4th Cir. 2022).

In light of the relevant precedent and the limited tower dump request in this case, we conclude that Appellant has not established a legitimate expectation of privacy concerning the information produced by AT&T. By their own terms, *Carpenter* and *Pacheco* were limited to CSLI data and forswore any application to tower dump requests. Moreover, the logical foundation in **Carpenter** and **Pacheco** extending Fourth Amendment privacy protection to CSLI is not present here; the data produced by AT&T did not reveal "a comprehensive chronicle of [Appellant's] physical movements," nor did it allow the government to track Appellant's "precise location and follow him continuously without detection." Pacheco, 263 A.3d at 641. Instead, law enforcement was merely able to "identif[y] phones near one location" namely, in the vicinity of T.S.'s house in Columbia County—"at one time" during the five-hour period on June 3, 2015 when she was attacked. **Adkinson**, 916 F.3d at 611 (emphasis in original); **see also Dunkins I**, 229 A.3d at 629. The tower dumps in the present matter were less a tool for "tracking" suspects and more akin to the "conventional surveillance technique[]" of "security cameras," capturing the identity of all cell phone users who happened to be in the vicinity of a crime scene. *Carpenter*, 138 S.Ct. at 2219-20; *see also Walker*, 2020 WL 4065980, at *8. Furthermore, the data provided by AT&T did not pinpoint Appellant to a specific building or location but instead only showed that his phone was within a range of up to seven and a half miles from T.S.'s rural home during the time period in question. *See* N.T. (Trial), at 565-76; *Carpenter*, 138 S.Ct. at 2211-12, 2219 (recognizing that, as population density increases in more urbanized areas, each cell sector correspondingly shrinks, and the location information from CSLI becomes more focused and revealing of the target's exact location); *cf. Dunkins I*, 229 A.3d at 625 & n.2 (campus police obtained log of a single wireless access point among 1,100 on college campus).¹⁵

In addition to challenging the propriety of the admission of the tower dump information under the Fourth Amendment, Appellant also argues that

_

¹⁵ Even if we found that the trial court erroneously denied suppression of the tower dump evidence, we would conclude that the error was harmless as the properly admitted and uncontradicted evidence—most notably Appellant's confession to the attempted kidnapping and rape of T.S., which was consistent with T.S.'s account of the incident—would overwhelm any prejudicial effect of the admission of the tower dump evidence such that it could not have contributed to the guilty verdict. **See Commonwealth v. Holt**, 273 A.3d 514, 540 (Pa. 2022) (error may be deemed harmless where, *inter alia*, "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"); **see also Commonwealth v. Petroll**, 738 A.2d 993, 1005-06 (Pa. 1999) (applying harmless error doctrine in suppression context).

the information was admitted in violation of his Sixth Amendment right to confrontation. Appellant contends that the cell tower evidence was left completely unverified and unauthenticated as the Commonwealth admitted the evidence through the testimony of PSP witnesses rather than an AT&T representative. As such, Appellant asserts that he was unable to cross-examine the contents of the information produced by AT&T in order to determine its authenticity.

Like Appellant's Sixth Amendment challenge to the admission of the Google search results, we must also find that Appellant has waived his Confrontation Clause argument with respect to the tower dump information based upon his failure to raise this issue at trial. When the Commonwealth sought the admission of the tower dump evidence, defense counsel stated his objection on the basis that "the standard records custodian wasn't here . . . [s]o, it is hearsay." N.T. (Trial), at 552. As Appellant did not raise the Confrontation Clause as grounds for his opposition to the admission of the tower dump evidence, he waived his appellate claim. *See Rosser*, 135 A.3d at 1087; *Akbar*, 91 A.3d at 235. 16

Having found that Appellant did not have a constitutionally protected privacy interest in the tower dump information and that he waived his

_

¹⁶ Furthermore, any argument Appellant would have on appeal related to the authentication of the tower dump evidence was waived as he did not object on that basis at trial. **See** Pa.R.E. 103(a)(1); **Wroten**, 257 A.3d at 742.

challenge to the admission of this evidence, Appellant's second appellate issue fails.

Consolidation

Appellant next argues that the trial court abused its discretion by denying his motion to sever and granting the Commonwealth's motion to consolidate the three separate cases, involving five victims. "[W]hether or not separate indictments should be consolidated for trial is within the sole discretion of the trial court and such discretion will be reversed only for a manifest abuse of discretion or prejudice and clear injustice to the defendant." **Commonwealth v. Cousar**, 928 A.2d 1025, 1037 (Pa. 2007) (citation omitted).

Appellant asserts that by allowing the cases to be tried together, the trial court allowed for the introduction of character or propensity evidence relating to one victim that would have been inadmissible if the cases were each tried separately. Appellant notes that the cases were disconnected in time and place, as they were spread out over five years and in various locations across three Pennsylvania counties. Appellant contends that the similarity of the five cases was only that they were of the "same class" of offenses, and even in that regard the cases were not entirely similar as three of the cases did not involve actual sexual assault. According to Appellant, the joint trial of the three indictments involving five separate incidents stripped him of his due process rights and prejudiced his defense.

Pursuant to Rule of Criminal Procedure 582, "[o]ffenses charged in separate indictments or informations may be tried together if . . . the evidence of each of the offenses would be admissible in a separate trial for the other and is capable of separation by the jury so that there is no danger of confusion." Pa.R.Crim.P. 582(A)(1)(a). Furthermore, under Rule 583, the trial court "may order separate trials of offenses or defendants, or provide other appropriate relief, if it appears that any party may be prejudiced by offenses or defendants being tried together." Pa.R.Crim.P. 583.

Reading these rules together, our Supreme Court established the following test for severance matters:

Where the defendant moves to sever offenses not based on the same act or transaction that have been consolidated in a single indictment or information, or opposes joinder of separate indictments or informations, the court must therefore determine: [1] whether the evidence of each of the offenses would be admissible in a separate trial for the other; [2] whether such evidence is capable of separation by the jury so as to avoid danger of confusion; and, if the answers to these inquiries are in the affirmative, [3] whether the defendant will be unduly prejudiced by the consolidation of offenses.

Commonwealth v. Ferguson, 107 A.3d 206, 210-11 (Pa. Super. 2015) (quoting **Commonwealth v. Collins**, 703 A.2d 418, 422 (Pa. 1997)).

Therefore, we must first assess whether the evidence of each of the offenses would be admissible in a separate trial for the others. *Id.* at 211. Generally, pursuant to Rule of Evidence 404, "[e]vidence of any other crime, wrong, or act is not admissible to prove a person's character in order to show that on a particular occasion the person acted in accordance with the

character." Pa.R.E. 404(b)(1). However, "[t]his evidence may be admissible for another purpose, such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident" and where "the probative value of the evidence outweighs its potential for unfair prejudice." Pa.R.E. 404(b)(2).

Under the common plan or scheme exception, evidence of other crimes or bad acts may be admitted where "the evidence reveals criminal conduct which is distinctive and so nearly identical as to become the signature of the same perpetrator." Commonwealth v. Tyson, 119 A.3d 353, 358-59 (Pa. Super. 2015) (en banc) (citation omitted). "Relevant to such a finding will be the habits or patterns of action or conduct undertaken by the perpetrator to commit crime, as well as the time, place, and types of victims typically chosen by the perpetrator." **Id.** at 359 (citation omitted). "Sufficient commonality of factors" between the incidents "dispels the notion that they are merely coincidental and permits the contrary conclusion that they are so logically connected they share a perpetrator." **Commonwealth v. Weakley**, 972 A.2d 1182, 1189 (Pa. Super. 2009). "If the evidence reveals that the details of each criminal incident are nearly identical, the fact that the incidents are separated by a lapse of time will not likely prevent the offer of the evidence unless the time lapse is excessive." Tyson, 119 A.3d at 359 (citation omitted).

We conclude that the five incidents here demonstrate sufficient similarity of plan and design that "evidence of each of the offenses would be

admissible in a separate trial for the other[s]." Ferguson, 107 A.3d at 210 (citation omitted). In his police interview, Appellant stated that he did not personally know any of his victims beforehand but instead saw them when driving by their houses or on Facebook and began a process of "scouting [them] out" in person and online. N.T. (Trial), at 707-08, 710, 712, 717-18, 722-23, 751, 781-82, 789, 798. Appellant entered the residences late at night or very early in the morning when he knew by the absence of other vehicles that only the intended target was at home. **Id.** at 718, 725, 732-36. He wore a hunting mask and gloves during the attacks and blindfolded and gagged the victims and zip tied their hands behind their backs. Id. at 727-29, 737, 756, 760, 775-78, 791-93, 804-05. Appellant then intended to transport the victims to another location—either a camper at a family camp site or his home—where he would rape them. **Id.** at 714, 765-66, 778-79, 794-95, 805. Appellant completed the rapes of K.M. and H.Z., he intended to transport D.S. and T.S. to another location to rape them but then suddenly realized what he was doing, and he entered A.H.'s house when he knew no one else was home with the intent to "[g]ag her." Id. at 709, 711, 714-16, 718-19, 724, 726-28, 806.

The evidence presented by the Commonwealth showed that Appellant had developed a "virtual signature" to the attacks. *Weakley*, 972 A.2d at 1189; *see also Commonwealth v. Miller*, 664 A.2d 1310, 1318-19 (Pa. 1995), *abrogated on other grounds by Commonwealth v. Hanible*, 836 A.2d 36 (Pa. 2003) (evidence of prior attempted rape and murder was

sufficiently similar to two rapes and murders for which defendant was on trial where evidence showed that all three incidents involved women of same race and body type who were lured into a car, taken to a remote area, raped, and severely beaten and bound afterwards); Tyson, 119 A.3d at 360-61 (sufficient factual similarities to show common plan or scheme where defendant invited two victims with similar appearance into his home, defendant knew victims were in a compromised state, and victims fell asleep and then woke up to discover that defendant had begun having vaginal intercourse with them while unconscious). Moreover, in light of the striking similarity of Appellant's pattern of behavior with respect to each of the victims, our conclusion that the evidence related to each incident would be admissible in trials for the others is not altered by the fact that Appellant's first and last attack were separated by five years. See Miller, 664 A.2d at 1319 (noting that "the importance of the time period [between the separate crimes] is inversely proportional to the similarity of the crimes in question" and holding that five-year period between attacks was not sufficiently lengthy to defeat admissibility in light of "the striking similarity of the three incidents"); **Tyson**, 119 A.3d at 361 (five-year period between two rapes did not support a finding of excessive time lapse to render evidence of past crime inadmissible).

Next, we must determine whether the evidence related to the five incidents was incapable of separation by the jury. Our Supreme Court has explained that "[w]here a trial concerns distinct criminal offenses that are distinguishable in time, space and the characters involved, a jury is capable

of separating the evidence." *Collins*, 703 A.2d at 423; *see also Ferguson*, 107 A.3d at 211. Here, the incidents occurred over a span of five years, and each involved a different victim and took place in a different location. Therefore, we find no basis to determine that the jury suffered confusion from the presentation of the evidence related to the various offenses.

Finally, we conclude that Appellant suffered no prejudice from the consolidation of these matters. For the purpose of this analysis, prejudice "is not simply prejudice in the sense that [the] appellant will be linked to the crimes for which he is being prosecuted, for that sort of prejudice is ostensibly the purpose of all Commonwealth evidence." Collins, 703 A.2d at 423 (citation omitted; emphasis in original). Instead, prejudice is established where the evidence only showed the appellant's "propensity to commit crimes, or because the jury was incapable of separating the evidence or could not avoid cumulating the evidence." **Id.** (citation omitted). In this case, the evidence of Appellant's five separate invasions of women's homes in order to rape and kidnap them did not simply show his propensity to commit crimes nor was the evidence unnecessarily cumulative; rather, Appellant engaged in a series of distinct, but remarkably similar attacks. Appellant "created the sequence of events and cannot fairly now demand that the . . . matters be severed and tried in separate trials." Ferguson, 107 A.3d at 212 (citation Therefore, we conclude that the trial court did not abuse its omitted). discretion in denying Appellant's motion to sever and granting the Commonwealth's motion to consolidate the informations.

Sentence

In his final issue, Appellant argues that his sentence of 59 to 280 years' imprisonment was excessive. Appellant contends that the trial court abused its discretion by failing to take into account several mitigating factors: his untreated psycho-sexual paraphilic disorder; his lack of a prior criminal record; and his prior military service. Appellant asserts that the aggregate sentence resulted in "a larger punishment than imposed in homicide cases." Appellant's Brief at 50. Appellant further argues that the term of incarceration was "essentially a life sentence without parole," and as such violated the prohibition on cruel and unusual punishment contained in the Eighth Amendment to United States Constitution. *Id.* at 49.

To the extent Appellant argues that his sentence was unconstitutional cruel and unusual punishment, this argument challenges the legality of the sentence. *Commonwealth v. Cartrette*, 83 A.3d 1030, 1042 (Pa. Super. 2013) (*en banc*). A claim that a sentence is illegal presents a pure question of law as to which our standard of review is *de novo*, and our scope of review is plenary. *Commonwealth v. Derrickson*, 242 A.3d 667, 673 (Pa. Super. 2020).

"The Eighth Amendment does not require strict proportionality between the crime committed and the sentence imposed; rather, it forbids only extreme sentences that are **grossly disproportionate** to the crime." **Commonwealth v. Lankford**, 164 A.3d 1250, 1252 (Pa. Super. 2017)

(emphasis in original).¹⁷ We apply a three-part test to determine whether an Eighth Amendment violation occurred:

[A] court's proportionality analysis under the Eighth Amendment should be guided by objective criteria, including (i) the gravity of the offense and the harshness of the penalty; (ii) the sentences imposed on other criminals in the same jurisdiction; and (iii) the sentences imposed for commission of the same crime in other jurisdictions.

Commonwealth v. Spells, 612 A.2d 458, 462 (Pa. Super. 1992) (en banc); see also Commonwealth v. Baker, 78 A.3d 1044, 1047 (Pa. 2013). "[A] reviewing court is not obligated to reach the second and third prongs of th[is] test unless 'a threshold comparison of the crime committed and the sentence imposed leads to an inference of gross disproportionality." Baker, 78 A.3d at 1047 (quoting Spells, 612 A.2d at 463).

We agree with the trial court that Appellant has not shown an inference that his sentence was grossly disproportionate to the crimes of which he was convicted. **See** Trial Court Opinion, 5/17/21, at 3. Appellant was charged with offenses relating to five separate attempted or completed rapes and kidnappings over a period of five years; in each of the cases, Appellant entered the victim's house surreptitiously late at night or early in the morning with the intent to surprise the victim, gag and bind her, and then violently rape her. As the trial court stated at sentencing, the circumstances of Appellant's

¹⁷ While Article I, Section 13 of the Pennsylvania Constitution also forbids the imposition of cruel punishment, this provision provides "no broader protections against cruel and unusual punishment than those extended under the Eighth Amendment." *Lankford*, 164 A.3d at 1252 (citation omitted).

attacks, even when he did not complete the assault, involved "unimaginable terror" for the five victims. N.T., 3/2/21, at 39. Appellant was convicted of 43 total offenses, including 24 first-degree felonies that are each punishable by up to 20 years' imprisonment. **See** 18 Pa.C.S. § 1103(1). While the trial court ran many of the sentences consecutively, it is well-established that the "imposition of consecutive rather than concurrent sentences lies within the sound discretion of the sentencing court." **Commonwealth v. Zirkle**, 107 A.3d 127, 133 (Pa. Super. 2013) (citation omitted). Because Appellant has not shown that the sentence imposed was grossly disproportionate to his crimes, we need not address the remaining two elements of the three-part test to assess whether his sentence was cruel or unusual. **See Baker**, 78 A.3d at 1047.

Turning to Appellant's argument that the trial court disregarded mitigating factors, we note that this claim implicates the discretionary aspect of his sentence. A challenge to the discretionary aspect of a sentence is not appealable as of right. *Commonwealth v. Akhmedov*, 216 A.3d 307, 328 (Pa. Super. 2019) (*en banc*). In order to invoke this Court's jurisdiction to consider a discretionary sentencing issue, the appellant must file a timely notice of appeal, preserve the issue at sentencing or in a post-sentence motion, and comply with Pa.R.A.P. 2119(f) by including a separate section in the appellate brief stating the reasons relied upon for the appeal. *Id.*

In this matter, Appellant filed a timely notice of appeal and included his present argument in his post-sentence motion; however, he did not include a

Pa.R.A.P. 2119(f) statement in his brief. Nevertheless, we will not find that Appellant has waived his discretionary sentencing claim based upon his lack of compliance with Rule 2119(f) as the Commonwealth did not object to Appellant's failure to adhere to the appellate rules. **See Commonwealth v. White**, 193 A.3d 977, 982 (Pa. Super. 2018).

We therefore must determine whether Appellant's sentencing claim constitutes a substantial question meriting our review; a substantial question exists when the appellant advances an argument that the sentence was inconsistent with a specific provision of the Sentencing Code or contrary to the fundamental norms underlying the sentencing process. *Akhmedov*, 216 A.3d at 328. Appellant has raised a substantial question here by pairing an excessive sentence claim with an assertion that the court failed to consider mitigating evidence. *Commonwealth v. Caldwell*, 117 A.3d 763, 770 (Pa. Super. 2015) (*en banc*).

Our standard of review for challenges to the discretionary aspects of sentencing is as follows:

Sentencing is a matter vested in the sound discretion of the sentencing judge, and a sentence will not be disturbed on appeal absent a manifest abuse of discretion. In this context, an abuse of discretion is not shown merely by an error in judgment. Rather, the appellant must establish, by reference to the record, that the sentencing court ignored or misapplied the law, exercised its judgment for reasons of partiality, prejudice, bias or ill will, or arrived at a manifestly unreasonable decision.

Commonwealth v. Taylor, 277 A.3d 577, 592-93 (Pa. Super. 2022) (citation omitted).

When imposing a sentence of incarceration, the court must consider the sentencing factors set forth in Section 9721(b), namely, "the protection of the public, the gravity of the offense as it relates to the impact on the life of the victim and on the community, and the rehabilitative needs of the defendant." 42 Pa.C.S. § 9721(b). The balance of the sentencing factors is the sole province of the sentencing court. *Commonwealth v. Miller*, 275 A.3d 530, 535 (Pa. Super. 2022). Furthermore, "the sentencing court, which is present at the hearing and observes all witnesses and the defendant firsthand, is in a superior position to review the defendant's character, defiance or indifference, and the overall effect and nature of the crime." *Id.* (citation and quotation marks omitted).

Appellant argues that the trial court ignored three mitigating factors when imposing its sentence: the fact that he had no prior criminal convictions; his prior military service; and his paraphilic disorder. However, the record reflects that each of these factors were discussed at the sentencing hearing. N.T., 3/2/21, at 12, 38. Moreover, the trial court reviewed Appellant's presentence investigative report ("PSI") prior to imposing the sentence. *Id.* at 18. "Where the sentencing court had the benefit of reviewing a PSI, we must presume that the sentencing judge was aware of relevant information regarding the defendant's character and weighed those considerations along with mitigating statutory factors." *Commonwealth v. Knox*, 165 A.3d 925, 930 (Pa. Super. 2017) (citation omitted). While Appellant argues that the trial court did not give sufficient weight to the cited mitigating factors, all the

J-S10032-22

Sentencing Code requires is that the court consider all of the relevant factors

when imposing the sentence. See Commonwealth v. Macias, 968 A.2d

773, 778 (Pa. Super. 2009) (appellate court cannot reweigh sentencing factors

and impose judgment in place of sentencing court where lower court was fully

aware of all mitigating factors).

Accordingly, Appellant is not entitled to relief on his discretionary

sentencing claim. Having found that each of Appellant's appellate issues lacks

merit, we therefore affirm his judgment of sentence.

Judgment of sentence affirmed.

Judgment Entered.

Joseph D. Seletyn, Esc

Prothonotary

Date: <u>04/28/2023</u>

- 45 -