[J-3-2021]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

BAER, C.J., SAYLOR, TODD, DONOHUE, DOUGHERTY, WECHT, MUNDY, JJ.

COMMONWEALTH OF PENNSYLVANIA,	:	No. 45 MAP 2020
	:	
Appellee	:	Appeal from the Order of the Superior Court dated February 12, 2020 at No. 1003 EDA 2019
v.	:	Affirming the Judgment of Sentence of the Northampton County Court of Common Pleas, Criminal Division,
ALKIOHN DUNKINS,	:	dated January 4, 2019 at No. CP-48-CR-1577-2017.
Appellant	:	
	:	ARGUED: March 9, 2021

OPINION

JUSTICE DOUGHERTY[1] **DECIDED: November 17, 2021**

We granted review to determine whether the trial court erred by denying suppression of wireless internet network (WiFi) connection records obtained by police without a warrant from the Information Technology Department of Moravian College. For the following reasons, we conclude this search was constitutionally permissible, and accordingly, we affirm the order of the Superior Court.

At approximately 2:00 a.m. on February 2, 2017, two masked men posed as campus police to gain entry to the dorm room shared by Greg Farina and William Reilley in the Hassler dormitory building on the Moravian College Campus in Bethlehem. The men held Farina and Reilley at gunpoint and stole $1,000 and a jar of marijuana from Reilley's footlocker. Reilley reported the robbery to campus officials around 11:00 a.m.

[1] The matter was reassigned to this author.

"APPENDIX A"

and, thereafter, campus police requested that Moravian College's Director of Systems Engineering, Christopher Laird, analyze its WiFi connection records to compile a list of students logged on to the WiFi in the Hassler building at the time of the robbery. Laird discovered only three Moravian College students were logged on to the campus WiFi at that location who did not reside in the Hassler building; two were females and the other was appellant, Alkiohn Dunkins.

Campus police relayed this information to Detective James Ruvolo of the Bethlehem Police Department. In the course of his investigation, Detective Ruvolo interviewed Reilley, appellant, and Colin Zarecki, another Moravian College student. Reilley told Detective Ruvolo he suspected appellant participated in the robbery because appellant previously stole from him by failing to pay for marijuana, while appellant denied being involved in the robbery and told Detective Ruvolo he had not entered the Hassler building since October 2016. Colin Zarecki told Detective Ruvolo that on February 3, 2017, the day after the robbery, appellant bragged to him about money he stole by posing as a campus police officer. Based on the above information, appellant was arrested and charged with robbery, conspiracy to commit robbery, receiving stolen property, and simple assault.[2]

Prior to trial, appellant filed a motion to suppress in which he claimed the campus police conducted an illegal search by obtaining the Hassler building WiFi connection records without a warrant. During a hearing on the motion, Laird testified Moravian College students access the college's WiFi network by entering their individual usernames and passwords, and that students may choose to have their devices automatically log on to the network without having to re-enter their username and

[2] 18 Pa.C.S. §3701(a)(1)(ii), 18 Pa.C.S. §903, 18 Pa.C.S. §3925(a), and 18 Pa.C.S. §2701(a)(1), respectively.

password each time they want WiFi access. The parties also acknowledged appellant assented to Moravian College's Computing Resources Policy. The policy provided:

> Logging in to or otherwise connecting to the campus network implies acceptance of this Moravian College . . . Policy[.]
>
> * * *
>
> The institution's computing equipment and network resources are dedicated to Moravian business to enhance and support the educational mission of Moravian College. These resources include all computers, workstations, and multi-user computer systems **along with local area networks and wireless networks** via the Internet.
>
> * * *
>
> [A]ny data transmitted over institutional assets or **connections made through institutional assets are included**. The institution has the right to inspect information stored on its system at any time, for any reason, and **users cannot and should not have any expectation of privacy with regard to any data, documents, electronic mail messages, or other computer files created or stored on computers within or connected to the institution's network**. All Internet data composed, transmitted, or received through the Internet's computer system is considered part of the institution's records and, as such, **subject at any time to disclosure to institutional officials, law enforcement, or third parties**[.]

Moravian College's Computing Resources Policy ("Computing Resources Policy") - Defense Exhibit 1 (emphasis added).[3] The trial court denied appellant's suppression motion and a jury later convicted him of the aforementioned charges. Thereafter, the trial court denied appellant's motion for extraordinary relief and sentenced him to an aggregate term of five to ten years' imprisonment. Following the denial of his post-sentence motion, appellant filed a direct appeal in the Superior Court.

In a unanimous, published opinion, a three-judge panel of the Superior Court affirmed the trial court's denial of suppression. *Commonwealth v. Dunkins*, 229 A.3d 622

[3] The Computing Resources Policy was included in Moravian's Student Handbook, which is provided to all students; all students must acknowledge they received and reviewed the handbook before enrolling at Moravian College.

(Pa. Super. 2020), *allocatur granted*, 237 A.3d 415 (Pa. 2020) (*per curiam*). The panel first rejected appellant's contention this case is controlled by *Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206 (2018). The panel ably explained the decision as follows:

> [In *Carpenter*,] the U.S. Supreme Court found law enforcement officials improperly acquired Carpenter's CSLI[4] without a warrant. In that case, Carpenter was a suspect in a string of armed robberies. Officers compelled Carpenter's wireless carriers to provide a record of Carpenter's historical CSLI for a four-month period, allowing the officers to track Carpenter's movements during the time when the robberies had occurred. *Carpenter*, 138 S.Ct. at 2212.
>
> Although the Court recognized an individual has a reduced expectation of privacy in information knowingly shared with another, the Court found the "nature of the particular documents sought" must be considered to determine whether there is a legitimate expectation of privacy. *Id.* at 2219. The Supreme Court recognized that modern cell phones generate time-stamped records known as CSLI when the phone continuously scans for the best signal from the closest cell site and connects to that cell site. *Id.* at 2211. Such information is collected by wireless carriers for business purposes to improve their network and to bill customers who incur "roaming" charges through another carrier's network. *Id.* The Supreme Court also noted that an electronic device will log CSLI simply through the user's operation of the phone on the carrier network "without any affirmative act on the part of the user beyond powering up." *Id.* at 2220.
>
> Emphasizing that "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society," the Supreme Court concluded that the officers invaded Carpenter's reasonable expectation of privacy in his physical movements by collecting the historical CSLI without a warrant as

---

[4] The *Carpenter* Court explained CSLI as follows:

> Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI).

Carpenter, 138 S.Ct. at 2211.

> the search provided "a comprehensive chronicle" of [Carpenter's] physical movements over a four-month period. *Id.* at 2211, 2219-20.
>
> However, while the Supreme Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," the Supreme Court pointed out that the holding in *Carpenter* was not simply about "using a phone" or "a person's movement at a particular time." *Id.* at 2217, 2220. Further, the Supreme Court emphasized that its decision was "narrow" and indicated that it was not expressing a view on real-time CSLI or "tower dumps" ("a download of information on all the devices that connected to a particular cell site during a particular interval"). *Id.* at 2220. The Supreme Court added 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.*

Dunkins, 229 A.3d at 628-29 (footnote omitted). In distinguishing *Carpenter*, the panel noted the "action by campus police in this case is akin to a 'tower dump' request as campus security sought general network connection information from one of Moravian's wireless access points near the location of the robbery at the time it occurred" and *Carpenter* specifically declined to invalidate "tower dump" requests. *Id.* at 629. To this point, the panel explained "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 Hassler dorm at the time of the robbery." *Id.*

The panel further opined, regardless of whether *Carpenter* was applicable to the present case, appellant's Fourth Amendment claim failed because he abandoned any purported expectation of privacy in the WiFi connection records due to the fact he consented to the Computing Resources Policy, which expressly authorizes the college to collect and disclose internet data "composed, transmitted, or received" through the campus WiFi. *Id.* at 630. The panel additionally relied on *Commonwealth v. Sodomsky*, 939 A.2d 363, 369 (Pa. Super. 2007), which held "[i]f a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy

in those contents" and federal case law holding "'[a] defendant can voluntarily consent in advance to a search as a condition of receiving contracted services.'" *Id.*, *quoting United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019), *cert. denied*, 139 S.Ct. 2762 (2019). The panel concluded appellant was not entitled to suppression of the WiFi connection records because he "agreed to surrender some privacy rights to have his cell phone access Moravian's WiFi network to assist him in his pursuit of a college degree" and he "was not required to log in or to maintain a constant connection to the campus WiFi network, but could have chosen to have his device access the internet through a wireless carrier or simply signed off the Moravian wireless network temporarily to avoid transmitting location data." *Id.* at 631.

We accepted review to consider the following question raised by appellant: "[w]hether the trial court erred by denying [appellant's] Motion to Suppress the cell site location information and/or his Motion for Extraordinary Relief requesting the same under the Fourth Amendment to the United States Constitution?" *Commonwealth v. Dunkins*, 237 A.3d 415 (Pa. 2020) (*per curiam*).

> Our standard of review over an order denying suppression requires us to consider only the Commonwealth's evidence and so much of the defense's evidence as remains uncontradicted when read in the context of the record as a whole. Where the record supports the suppression court's factual findings, we are bound by those facts and may reverse only if the legal conclusions drawn therefrom are in error. However, as here, where the appeal turns on allegations of legal error, the suppression court's conclusions of law are not binding as it is this Court's duty to determine if the suppression court properly applied the law to the facts. As such, the legal conclusions of the lower courts are subject to our plenary review.

In Interest of A.A., 195 A.3d 896, 901 (Pa. 2018) (internal citations, quotations, and ellipses omitted). Embedded in the parties' arguments is the interesting and novel issue of whether *Carpenter* extends to the WiFi connection records appellant sought to suppress in the present case. Before reaching that particular question, however, we must

first determine the dispositive issue of whether appellant abandoned any purported expectation of privacy in the WiFi connection records by consenting to the college's Computing Resources Policy.[5]

Appellant contends he did not abandon a reasonable expectation of privacy in the WiFi connection records because his consent to the Computing Resources Policy was not fully voluntary but instead constituted mere acquiescence to a show of authority by Moravian College. In doing so, appellant relies on *Carpenter*, which "stated that by a user consenting to share some data, 'in no meaningful sense does the user voluntarily assume[ ] the risk of turning over a comprehensive dossier of his physical movements.'" Appellant's Brief at 56, *quoting Carpenter*, 138 S.Ct. at 2220. Affirming the Superior Court

---

[5] Respectfully, we did not grant allocatur in this case, as Justice Wecht alleges, "to decide whether *Carpenter*'s expectation-of-privacy ruling extends to records that are created when a college student uses an internet-capable device to connect automatically to a college's campus-wide Wi-Fi network." Concurring and Dissenting Opinion at 2. Instead, we granted review of this specific question: "Whether the trial court erred by denying [appellant's] Motion to Suppress the cell site location information and/or his Motion for Extraordinary Relief requesting the same under the Fourth Amendment to the United States Constitution[?]" *Commonwealth v. Dunkins*, 237 A.3d 415 (Pa. 2020) (*per curiam*). While we recognize the constitutional issue regarding the applicability of *Carpenter* is subsumed in that question, we find it prudent to answer the question in the negative by holding appellant abandoned any purported expectation of privacy in the WiFi connection records. "By reaching our holding on these grounds, we not only resolve [appellant's] claim on the terms in which he has framed it, we also 'adhere to the sound tenet of jurisprudence that courts should avoid constitutional issues when the issue at hand may be decided upon other grounds.'" *Commonwealth v. Herman*, 161 A.3d 194, 209 (Pa. 2017), *quoting In re Fiori*, 673 A.2d 905, 909 (Pa. 1996) (citation omitted); *accord Ala. State Fed'n of Labor v. McAdory*, 325 U.S. 450, 461-62 (1945) ("It has long been [a] considered practice not to decide abstract, hypothetical or contingent questions, or to decide any constitutional question in advance of the necessity for its decision, or to formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied, or to decide any constitutional question except with reference to the particular facts to which it is to be applied[.]") (internal citations omitted). To first address the hypothetical question of whether an individual may or may not possess, under the Fourth Amendment, an expectation of privacy in data that is transmitted over WiFi networks would abandon that practice.

on this issue, appellant claims, "would invalidate [*Carpenter*] and would give law enforcement an end-run around judicial oversight" leading to "omnipresent government surveillance for any Pennsylvanian who uses a third party to connect to the internet." *Id.* at 56-57. Lastly, appellant contends his assent to the Computing Resources Policy did not constitute abandonment of his expectation of privacy with regard to his whereabouts because "[t]he plain language of the policy does not inform a reader that he/she is consenting to unfettered government access to their history of movements." *Id.* at 57.[6]

The Commonwealth responds by arguing appellant voluntarily relinquished any expectation of privacy with respect to all information transmitted through Moravian's WiFi network, including his location, when he assented to the Computing Resources Policy, which specifically stated the information could be disclosed to law enforcement. Supporting this theory, according to the Commonwealth, is the fact that appellant affirmatively chose to have his cell phone connected to Moravian's WiFi, and committed the armed robbery while being logged on to the network with his username and password. The Commonwealth further contends the present case is akin to *Adkinson*, in which the Seventh Circuit Court of Appeals held a defendant's Fourth Amendment rights were not violated because he consented to the collecting and sharing of "tower dumps" by a third

---

[6] In their brief supporting appellant, *amicus curiae* American Civil Liberties Union, American Civil Liberties Union of Pennsylvania, and the Electronic Frontier Foundation (collectively referred to hereinafter as "ACLU") also contend appellant's consent to the Computing Resources Policy did not constitute abandonment of his reasonable expectation of privacy in the WiFi connection records. ACLU argues appellant did not voluntarily consent to the WiFi connection records being disclosed to law enforcement because the Computing Resources Policy did not mention location tracking. *See* ACLU Brief at 26. In any event, ACLU contends terms of service, which are non-negotiable and regularly developed by service providers, do not determine an individual's Fourth Amendment rights because the user has no choice but to agree. *Id.* at 26-29, *citing Carpenter*, 138 S.Ct. 2219-20 and *Byrd v. United States*, ___ U.S. ___, 138 S.Ct. 1518 (2018) (driver has reasonable expectation of privacy in rental car even where car driven in violation of rental agreement).

party, T-Mobile. As such, the Commonwealth argues "[a]ppellant relinquished any possessory rights with regard to this information to a third party, Moravian College, and had no legitimate expectation of privacy." Commonwealth's Brief at 18.[7]

The Fourth Amendment to the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" U.S. CONST. amend. IV. To prevail on a suppression motion implicating the Fourth Amendment, "a defendant must demonstrate a legitimate expectation of privacy in the area searched or effects seized, and such expectation cannot be established where a defendant has meaningfully abdicated his control, ownership or possessory interest." *Commonwealth v. Dowds*, 761 A.2d 1125, 1131 (Pa. 2000), *citing Commonwealth v. Hawkins*, 718 A.2d 265, 267 (Pa. 1998). "The theory of abandonment is predicated upon the clear intent of an individual to relinquish control of the property he possesses [and] . . . is primarily a question of intent, [which] may be

---

[7] The Office of the Attorney General of Pennsylvania (OAG) and the Pennsylvania District Attorneys Association (PDAA) filed *amicus curiae* briefs in support of the Commonwealth. OAG claims appellant's arguments miss the mark because consent to search is irrelevant when there is no reasonable expectation of privacy and appellant did not abandon his alleged expectation of privacy in acquiescence to a show of authority as he could have used his own cell service rather than connecting to Moravian's WiFi if he did not want to share his location information. For this same reason, OAG agues *Carpenter* did not hold such acknowledgements to be invalid because the defendant in Carpenter had no choice but to share his location while appellant did have a choice. Regarding ACLU's argument that the Computing Resources Policy did not provide a warning about location data, OAG notes there is universal knowledge that cell phone data includes location data. OAG also disputes ACLU's arguments that: 1) the Computing Resources Policy did not empower the police to collect the WiFi connection records because the acknowledgment specifically provided that such information could be turned over to law enforcement; and 2) the acknowledgement is invalid under *Byrd* because *Byrd* had nothing to do with a specific signed denial of an expectation of privacy and only held a driver in lawful possession of a rental car did not lack an expectation of privacy because his name was not on the rental agreement. PDAA joins in the arguments by the Commonwealth and OAG that "appellant explicitly consented to allow Moravian College to release information regarding his connections to Moravian's network by signing the computing policy within Moravian College's Student Handbook." PDAA's Brief at 13.

inferred from words spoken, acts done, and other objective facts." *Commonwealth v. Shoatz*, 366 A.2d 1216, 1219-20 (Pa. 1976) (internal citation omitted). Further, "[a]ll relevant circumstances existing at the time of the alleged abandonment should be considered" and "[t]he issue is . . . whether the person prejudiced by the search had voluntarily discarded, left behind, or otherwise relinquished his interest in the property in question so that he could no longer retain a reasonable expectation of privacy with regard to it at the time of the search." *Id.* at 1220 (internal citations omitted).

By assenting to the Computing Resources Policy and logging on to the Moravian College WiFi network on his cell phone thereafter, appellant specifically agreed he "cannot and should not have any expectation of privacy with regard to any data . . . created or stored on computers within or connected to the institution's network." Computing Resources Policy. Appellant further agreed "[a]ll Internet data composed, transmitted, or received through the institution's computer system is considered part of the institution's records and, as such, subject at any time to disclosure to institutional officials, law enforcement, or third parties[.]" *Id.* These acts by appellant provide clear intent to relinquish any purported expectation of privacy in the WiFi connection records.[8, 9] Furthermore, this abandonment by appellant was voluntary. Although appellant was

---

[8] We reject the argument forwarded by appellant and ACLU that he did not assent to the disclosure of his location information because the Computing Resources Policy did not specifically warn that "data" includes location data. As stated succinctly by the OAG, "[s]uch an argument might have had force a decade age, but as cell phone usage has become universal, so has common knowledge of how they work." OAG's Brief at 24, *citing, e.g.*, *Commonwealth v. Almonor*, 120 N.E.3d 1183, 1195 (Mass. 2019) (society has "reasonably come to expect that the voluntary use of cell phones -- such as when making a phone call -- discloses cell phones' location information to service providers . . . and that records of such calls may be maintained") (citation omitted).

[9] Justice Wecht faults us for assuming the Computing Resources Policy agreed to by appellant was legally binding. While appellant argues his consent to the policy did not constitute a consent to search, *see* Appellant's Brief at 55-57, he does not challenge the validity or enforceability of the policy. Therefore, the policy is legally binding for purposes

required to assent to the Computing Resources Policy and other policies in the Student Handbook prior to enrolling at Moravian College, he further acquiesced to the consequences of the Computing Resources Policy upon "[l]ogging in to or otherwise connecting to the campus network[.]" *Id.* Nothing in the Computing Resources Policy required appellant to log on to Moravian's WiFi network on his cell phone and remain connected on that device at all times, but he did so voluntarily.[10] Accordingly, we have little difficulty concluding appellant abandoned any purported expectation of privacy in the WiFi connection records and his suppression motion was properly denied. We therefore affirm the order of the Superior Court.

Chief Justice Baer and Justices Saylor, Todd and Mundy join the opinion.

Justice Wecht files a concurring and dissenting opinion in which Justice Donohue joins.

Judgment Entered 11/17/2021

Elizabeth Zisk
CHIEF CLERK

---

of this appeal. *See Valentino v. Philadelphia Triathlon, LLC*, 209 A.3d 941, 956 (Pa. 2019) (Donohue, J., Opinion in Support of Reversal) ("Here, Appellant does not challenge the validity or the enforceability of the contractual assumption of risk in the survival action she brought (as administratix) on behalf of Decedent's estate. Therefore, for purposes of this appeal, the liability waiver is valid and enforceable as a complete defense to the survival action.").

[10] To be clear, we do not "contemplate[ ] just one fact" in holding appellant voluntarily abandoned any purported expectation of privacy in the WiFi connection records as Justice Wecht suggests. Concurring and Dissenting Opinion at 34. Our analysis recognizes Moravian College required appellant to sign the Computing Resources Policy, which outlined the consequences of using the WiFi network. However, our analysis also takes into consideration the fact that appellant then voluntarily used the WiFi network on his cell phone. Those two facts, taken together, constitute a voluntary abandonment of any purported expectation of privacy in the WiFi connection records.

2020 PA Super 38

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF PENNSYLVANIA
v.	:	
ALKIOHN DUNKINS	:	
Appellant	:	No. 1003 EDA 2019

Appeal from the Judgment of Sentence Entered January 4, 2019
In the Court of Common Pleas of Northampton County Criminal Division
at No(s): CP-48-CR-0001577-2017

BEFORE: PANELLA, P.J., STABILE, J., and STEVENS, P.J.E.*

OPINION BY STEVENS, P.J.E.: **FILED FEBRUARY 12, 2020**

Appellant Alkiohn Dunkins appeals the judgment of sentence entered by the Court of Common Pleas of Northampton County after a jury convicted Appellant of Robbery, Conspiracy to Commit Robbery, Receiving Stolen Property, and Simple Assault.[1] Appellant claims the trial court erred in refusing to suppress wireless internet connection records that were obtained by campus police at Moravian College in a warrantless search. Appellant also challenges the sufficiency and weight of the evidence supporting his convictions. We affirm.

On February 2, 2017, at approximately 2:00 a.m., on the Moravian College campus in Bethlehem, Pennsylvania, two men wearing ski masks pretended to be campus police to gain access to the dorm room shared by Greg Farina and William Reilley, a Moravian student known to sell marijuana

---

* Former Justice specially assigned to the Superior Court.
[1] 18 Pa.C.S.A. §§ 3701(a)(1)(ii), 903, 3925(a), and 2701(a)(1), respectively.

"APPENDIX B"

on campus. Notes of Testimony ("N.T."), Trial, 9/4/18, at 31-38; 9/5/18, at 152-57. When Farina opened the dorm door, one of the masked men punched Farina, causing him to fall. ***Id.*** The masked men held the students at gunpoint and demanded marijuana and the key to Reilley's footlocker. ***Id.*** The masked men accessed the footlocker and took approximately $1,000 in cash as well as a jar of marijuana. ***Id.*** Before leaving the dorm, the perpetrators hit Reilley and Farina on the sides of their heads. ***Id.***

Several hours later, around 11 a.m., Reilley reported the robbery to campus officials. N.T., 9/4/18, at 39-40; 9/5/18, at 159. Campus Police Officer Thomas Appleman requested that Moravian's Director of Systems Engineering, Christopher Laird, analyze its wireless network (WiFi) data to compile a list of the students logged on to the network near the wireless access point in the dormitory building where Reilley and Farina resided.[2] N.T., Pre-trial motion Hearing, 4/19/18, at 40-43; N.T. Trial, 9/5/18, at 215-19. Campus officials discovered, at the time of the robbery, there were only three individuals logged onto the campus WiFi at that location that did not reside in that building. N.T., 9/5/18, at 218-19. Two of the three WiFi users were female. The male user was Appellant, who was also a Moravian student. N.T. Hearing, 4/19/18, at 44, N.T. 9/5/18, at 219.

---

[2] Laird indicated that Moravian utilizes approximately 1,100 wireless network access points placed throughout the campus in order to offer its students and faculty nearly seamless Internet connection. N.T., 4/19/18, at 27-29.

Thereafter, Officer Appleman provided this data to Detective James Ruvolo of the Bethlehem Police Department, who took over the investigation. Reilley told Detective Ruvolo that Appellant previously "robbed" him by taking marijuana from him without payment in return. N.T., 9/4/18, at 41, 49. When Appellant was interviewed, he denied being in the Hassler dormitory since October 2016. ***Id***. at 54.

Colin Zarzecki, who lived in in the dorm room next to Appellant's, told police that Appellant came to his room after midnight on February 3, 2017, "fanned out" a display of cash, and bragged that he obtained this money in a recent robbery. N.T., 9/5/18, at 102, 107. Appellant boasted that he and another individual posed as campus police officers to gain access to the victim's room and subsequently stole drugs and money from the victim's footlocker. ***Id***. at 102-105, 124-25.

After Appellant was arrested and charged with the aforementioned offenses, Appellant filed a suppression motion, arguing that the campus police conducted an illegal search in obtaining the campus WiFi log-on data without first obtaining a warrant. At one of the suppression hearings held by the trial court, Moravian Systems Engineering Director Laird explained that, in order to utilize Moravian campus WiFi, each student must log on to the network with their individual username and password. However, at their initial log-on, students may choose to have their devices automatically log on to the campus WiFi without entering their credentials again. N.T., 4/19/18, at 27.

The parties also noted that Appellant had signed the Moravian Student Handbook when enrolling at the college, indicating that he accepted and understood Moravian's policies, including the following technology rules:

> Logging in to or otherwise connecting to the campus network implies acceptance of this Moravian College ... Policy. ...
>
> ***
>
> The institution's computing equipment and network resources are dedicated to Moravian business to enhance and support the educational mission of Moravian College. These resources include all computers, workstations, and multi-user computer systems *along with local area networks and wireless networks* via the Internet.
>
> ***
>
> [A]ny data transmitted over institutional assets or *connections made through institutional assets are included.* The institution has the right to inspect information stored on its system at any time, for any reason, and *users cannot and should not have any expectation of privacy with regard to any data*, documents, electronic mail messages, or other computer files *created or stored on computers within or connected to the institution's network*. All Internet data composed, transmitted, or received through the Internet's computer system is considered part of the institution's records and, as such, *subject at any time to disclosure to institutional officials, law enforcement, or third parties*...

N.T. 4/19/18, at 10-23; Defense Exhibit 1 (emphasis added). On April 26, 2018, the trial court denied Appellant's suppression motion.

At the conclusion of Appellant's trial, on September 5, 2018, the jury convicted Appellant of Robbery, Conspiracy to Commit Robbery, Receiving Stolen Property, and Simple Assault. On November 21, 2018, Appellant filed a motion for extraordinary relief, which was subsequently denied. On January 4, 2019, the trial court imposed an aggregate sentence of five to ten years'

imprisonment. On January 10, 2019, Appellant filed a post-sentence motion, which the trial court denied on March 1, 2019. Appellant filed a timely notice of appeal on March 19, 2019 and complied with the trial court's direction to file a Concise Statement of Errors Complained of on Appeal pursuant to Pa.R.A.P. 1925(b).

Appellant raises the following issues for our review on appeal:

> 1. Whether the Court erred by denying [Appellant's] Motion to Suppress the cell site location information purportedly tracking his cellphone and/or his Motion for Extraordinary Relief requesting the same?
>
> 2. Whether the evidence at trial was insufficient to sustain the Commonwealth's burden with respect to all charges as there was insufficient evidence to indicate that [Appellant] conspired with another to commit the instant offense?
>
>   a. Whether there was sufficient evidence as to [Appellant's] identity as one of the perpetrators and/or conspirators?
>
> 3. Whether the verdict was against the weight of the evidence as while there was evidence that [Appellant's] cell phone was in the vicinity of the Robbery, there was no evidence that [Appellant] had the phone at the time of the Robbery nor was there any evidence that [Appellant] was present at the scene and the witness who proffered that [Appellant] admitted to a Robbery was unworthy of belief?

Appellant's Brief, at 10.

We first review Appellant's claim that the trial court erred in denying his suppression motion. Our standard of review is as follows:

> Our standard of review in addressing a challenge to the denial of a suppression motion is limited to determining whether the suppression court's factual findings are supported by the record and whether the legal conclusions drawn from those facts are correct. Because the Commonwealth prevailed before the

> suppression court, we may consider only the evidence of the Commonwealth and so much of the evidence for the defense as remains uncontradicted when read in the context of the record as a whole. Where the suppression court's factual findings are supported by the record, we are bound by these findings and may reverse only if the court's legal conclusions are erroneous. Where, as here, the appeal of the determination of the suppression court turns on allegations of legal error, the suppression court's legal conclusions are not binding on an appellate court, whose duty it is to determine if the suppression court properly applied the law to the facts. Thus, the conclusions of law of the courts below are subject to our plenary review.

Commonwealth v. Mbewe, 203 A.3d 983, 986 (Pa.Super. 2019) (citations and quotation marks omitted). In addition, "our scope of review from a suppression ruling is limited to the evidentiary record that was created at the suppression hearing." ***Commonwealth v. Rapak***, 138 A.3d 666, 670 (Pa.Super. 2016) (*citing* ***In re L.J.***, 622 Pa. 126, 79 A.3d 1073, 1087 (2013)).

Appellant contends the campus police conducted an illegal search by accessing Moravian's wireless internet connection records without first obtaining a warrant. Appellant claims the officers invaded his right to privacy in his physical movements through cell site location information (CSLI).

The Fourth Amendment of the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV.[3] Our courts

---

[3] While not explicitly stated in the record, the parties agree that Moravian Police Officer Appleman was deemed a state actor subject to the Fourth Amendment as he acted as an agent of the state in accessing the college's wireless information. ***See Commonwealth v. Yim***, 195 A.3d 922, 927 (Pa.Super. 2018), *appeal denied*, 204 A.3d 919 (Pa. 2019) (quoting ***Burdeau v. McDowell***, 256 U.S. 465, 475, 41 S.Ct. 574, 65 L.Ed. 1048 (1921))

have recognized that "[t]he protection of the Fourth Amendment does not depend on a property right in the invaded place but does depend on whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place. ***Commonwealth v. Cruz***, 166 A.3d 1249, 1254 (Pa.Super. 2017) (quoting ***Commonwealth v. Brundidge***, 533 Pa. 167, 172–73, 620 A.2d 1115, 1118 (1993)).[4]

Appellant claims this case is controlled by ***Carpenter v. U.S.***, ___U.S.___, 138 S.Ct. 2206 (U.S. June 22, 2018), in which the U.S. Supreme Court found law enforcement officials improperly acquired Carpenter's CSLI without a warrant. In that case, Carpenter was a suspect in a string of armed robberies. Officers compelled Carpenter's wireless carriers to provide a record of Carpenter's historical CSLI for a four-month period, allowing the officers to

---

(emphasizing that "[t]he Fourth Amendment's protection against unlawful searches and seizures applies only to actions by the government, as "[i]ts origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority[.]"

At the suppression hearing, Officer Appleman indicated that as a Moravian College campus police officer, he was responsible for ensuring campus safety and investigating crimes. N.T., 4/19/18, at 58. Officer Appleman indicated that all Moravian police officers have Act 120 certification (or an applicable waiver) and are permitted to carry firearms, make arrests, and initiate criminal proceedings. ***Id.*** at 58-60. Officer Appleman indicated that campus officers were permitted to take any action "that a police officer for a municipality or a state policeman could do." ***Id.*** at 59.

[4] Appellant has not argued that he is entitled to greater protection under the Pennsylvania Constitution. ***See Commonwealth v. Edmunds***, 526 Pa. 374, 586 A.2d 887, 895 (1991) (setting forth a four-factor analysis which an appellant must analyze to present a claim for higher protection under the Pennsylvania Constitution).

track Carpenter's movements during the time when the robberies had occurred.[5] ***Carpenter***, 138 S. Ct. at 2212.

Although the Court recognized an individual has a reduced expectation of privacy in information knowingly shared with another, the Court found the "nature of the particular documents sought" must be considered to determine whether there is a legitimate expectation of privacy. ***Id***. at 2219. The Supreme Court recognized that modern cell phones generate time-stamped records known as CSLI when the phone continuously scans for the best signal from the closest cell site and connects to that cell site. ***Id***. at 2211. Such information is collected by wireless carriers for business purposes to improve their network and to bill customers who incur "roaming" charges through another carrier's network. ***Id***. The Supreme Court also noted that an electronic device will log CSLI simply through the user's operation of the phone on the carrier network "without any affirmative act on the part of the user beyond powering up." ***Id***. at 2220.

Emphasizing that "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society," the Supreme Court concluded that the officers invaded Carpenter's reasonable expectation of privacy in his physical

---

[5] Law enforcement in ***Carpenter*** obtained court orders to access to this CSLI without a warrant under the Stored Communications Act which allowed the government to request certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought are "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d).

movements by collecting the historical CSLI without a warrant as the search provided "a comprehensive chronicle" of the appellant's physical movements over a four-month period. ***Id***. at 2211, 2219-20.

However, while the Supreme Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," the Supreme Court pointed out that the holding in ***Carpenter*** was not simply about "using a phone" or "a person's movement at a particular time." ***Id***. at 2217, 2220. Further, the Supreme Court emphasized that its decision was "narrow" and indicated that it was not expressing a view on real-time CSLI or "tower dumps" ("a download of information on all the devices that connected to a particular cell site during a particular interval"). ***Id***. at 2220. The Supreme Court added 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 this case, Appellant fails to acknowledge the ***Carpenter*** decision did not invalidate "tower dump" requests by law enforcement to identify all of the devices that were connected to one particular cell site during a particular interval. This action by campus police in this case is akin to a "tower dump" request as campus security sought general network connection information from one of Moravian's wireless access points near the location of the robbery at the time it occurred.

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 Hassler dorm at the time of the robbery. Using the process of elimination, campus officials were able to determine that, at the time of the robbery, Appellant was the only male student logged on to campus WiFi at the Hassler dorm who did not reside in that location.

Appellant also does not appreciate the difference between the CSLI obtained in ***Carpenter*** and the WiFi data obtained in this case. Whereas CSLI tracks an individual's movements at all times of the day regardless of where he travels, the WiFi data in this case is only collected when an individual logs onto the campus wireless network and is present on the Moravian campus.

We agree with the trial court's observation that the Moravian WiFi network is confined to the college campus and offered as an available option to students and faculty. When college officials seek to determine which students are logged on to the network near a particular wireless access point at a particular time, the private wireless network functions similarly to a security camera that may exist at the college. As such, the decision in ***Carpenter*** does not invalidate the warrantless search in this case.[6]

---

[6] In attempting to suppress the limited wireless network information obtained in this case, Appellant does not recognize the distinction between a specific request for a compilation of an individual's historical CSLI and a general request for "tower dump" information or similar data from a particular cell

Moreover, Appellant cannot reasonably argue that he was subjected to an illegal warrantless search under the Fourth Amendment when he specifically consented to Moravian's internet use policy, which clearly stated that individuals who choose to utilize the campus computer system and wireless network provide authorization for the college to collect and disclose all internet data composed, transmitted, or received through the campus computer system and its network connections.

This Court has held that "[i]f a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents." ***Commonwealth v. Sodomsky***, 939 A.2d 363, 369 (Pa.Super. 2007). ***See also U.S. v. Simons***, 206 F.3d 392 (4th Cir. 2000) (finding employee had no legitimate expectation of privacy in his internet activity when the employer's policy clearly stated that all internet activity would be audited, inspected, and monitored by the employer).

Moreover, other jurisdictions have recognized that "[a] defendant can voluntarily consent in advance to a search as a condition of receiving

---

tower or wireless access point for a particular time. Appellant does not specifically argue that the decision in ***Carpenter***, which the Supreme Court characterized as "narrow," should be extended to require law enforcement to obtain a warrant before seeking "tower dump" information or similar requests. In the absence of meaningful analysis from Appellant on this issue, we decline to review this issue further. ***See Commonwealth v. Roney***, 622 Pa. 1, 28, 79 A.3d 595, 610 n. 12 (2013) (finding sub-issue to be waived for lack of development with argument, citation to authority, or analysis).

contracted services." ***United States v. Adkinson***, 916 F.3d 605, 610 (7th Cir. 2019), *cert. denied*, 139 S. Ct. 2762, 204 L. Ed. 2d 1146 (2019) (citing ***Medlock v. Trustees of Indiana University***, 738 F.3d 867 (7th Cir. 2013)).[7]

In ***Adkinson***, the United States Court of Appeals for the Seventh Circuit found that the appellant provided voluntary consent to a search of his cell-site information as a condition of using a phone serviced by T-Mobile, as the parties' use agreement authorized T-Mobile to disclose such information "when reasonably necessary to protect its rights, interests, property, or safety, or that of others." ***Id***. As such, the Seventh Circuit found T-Mobile was permitted to give law enforcement "tower dump" information it obtained from cell sites near one of its stores that was robbed at gunpoint.[8] ***Id***.

---

[7] We consider the ***Simons***, ***Adkinson***, and ***Medlock*** decisions from federal circuit courts to be persuasive authority. This Court has provided that:

> absent a United States Supreme Court pronouncement, the decisions of federal courts are not binding on Pennsylvania state courts, even when a federal question is involved. When considering a given issue, however, we prefer Third Circuit decisions to those of other federal circuits, to discourage litigants from 'crossing the street' to obtain a different result in federal court than they would in Pennsylvania court. If, however, the Third Circuit has no law on a given question, we may seek guidance in the courts of appeals and district courts in other circuits.

Graziani v. Randolph, 856 A.2d 1212, 1218 (Pa.Super. 2004) (quoting ***Werner v. Plater-Zyberk,*** 799 A.2d 776, 782 (Pa.Super. 2002)).

[8] The Seventh Circuit also found that T-Mobile's disclosure of CSLI to law enforcement was permissible under the private search doctrine and was not invalidated by the decision in ***Carpenter***, which did not apply warrantless "tower dump" requests. ***Adkinson***, 916 F.3d at 611.

Similarly, in ***Medlock***, the Seventh Circuit reasoned that Medlock had not been subjected to an illegal search of his dorm room by resident leadership when he had given explicit consent to have his room searched for contraband and other evidence for any violations of the health and safety codes as a condition of Medlock being permitted to live in an on-campus dormitory. ***Medlock***, 738 F.3d at 872 (7th Cir. 2013) (observing that Medlock could have lived off campus but instead "chose to trade some privacy for a dorm room").

Likewise, prior to the robbery in this case, Appellant signed a "Computing Resources" policy indicating that he understood that, in exchange for the privilege of accessing Moravian's WiFi network, Moravian had the right to collect, inspect, and share internet data transmitted over institutional assets or connections made through institutional assets. N.T. 4/19/18, at 10-23; Defense Exhibit 1. The policy explicitly stated that "logging into or otherwise connecting to the campus network implies acceptance of this Moravian ... Policy." ***Id.***

We agree with the trial court's finding that the plain language of the policy "informs users of the campus wireless network that any connections made to that network are subject to inspection by the College at any time, as well as disclosure to law enforcement, and that users have no expectation of privacy in that electronic information." Trial Court Opinion, 4/26/18, at 3.

As such, Appellant agreed to surrender some privacy rights to have his cell phone access Moravian's WiFi network to assist him in his pursuit of a college degree at Moravian. Appellant was not required to log in or to maintain

a constant connection to the campus WiFi network, but could have chosen to have his device access the internet through a wireless carrier or simply signed off the Moravian wireless network temporarily to avoid transmitting location data. For the foregoing reasons, Appellant was not entitled to suppression of the wireless network data that was lawfully obtained by campus police.

Appellant also challenges the sufficiency of the evidence supporting his convictions. Our standard of review is as follows:

> The standard we apply in reviewing the sufficiency of the evidence 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 [that of] 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 trier 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. Leaner, 202 A.3d 749, 768, (Pa.Super. 2019) (citation omitted). To reiterate, the jury, as the trier of fact—while passing on the credibility of the witnesses and the weight of the evidence—is free to believe all, part, or none of the evidence. ***Commonwealth v. Melvin***, 103 A.3d 1, 39 (Pa. Super. 2014) (citation omitted). In conducting review, the appellate court

> may not weigh the evidence and substitute its judgment for the fact-finder. ***Id.*** at 39-40.

Commonwealth v. Baumgartner, 206 A.3d 11, 14–15 (Pa.Super. 2019).

As noted above, Appellant was convicted of robbery, conspiracy to commit robbery, and related offenses. To sustain a robbery conviction, the Commonwealth must show that the defendant "in the course of committing a theft, ... threatens another with or intentionally puts him in fear of immediate serious bodily injury." 18 Pa.C.S.A. § 3701(a)(1)(ii). Further, criminal conspiracy is defined as follows:

> A person is guilty of conspiracy with another person or persons to commit a crime if with the intent of promoting or facilitating its commission he:
>
> > (1) agrees with such other person or persons that they or one or more of them will engage in conduct which constitutes such crime or an attempt or solicitation to commit such crime; or
> >
> > (2) agrees to aid such other person or persons in the planning or commission of such crime or of an attempt or solicitation to commit such crime.

18 Pa.C.S.A. § 903.

Appellant specifically claims there was insufficient evidence to show he was one of the perpetrators who committed the charged crimes, as the prosecution could not definitively prove Appellant was the individual that was in possession of his phone near the victim's dorm at the time of the robbery. Appellant asserts that the Commonwealth was required to present records of calls or text messages to prove that Appellant was the individual in possession of the phone during the relevant time period.

We acknowledge that "cellular phones are not always exclusively used by the person to whom the phone number is assigned." ***Commonwealth v. Koch***, 39 A.3d 996, 1005 (Pa.Super. 2011). However, as noted above, a perpetrator's identity may be established with circumstantial evidence. ***Baumgartner***, ***supra***. This Court has recognized that "[e]vidence of identification need not be positive and certain to sustain a conviction." ***Commonwealth v. Ovalles***, 144 A.3d 957, 969 (Pa.Super. 2016) (citing ***Commonwealth v. Jones,*** 954 A.2d 1194, 1197 (Pa.Super. 2008)).

As noted above, Appellant was considered a suspect in the target offenses after Moravian network access records revealed that Appellant was the only male student who did not reside in the Hassler dorm that had a device signed onto the Moravian WiFi network on that particular network access point at the time of the robbery.

The prosecution presented additional evidence to corroborate the identity of the individual in possession of Appellant's cellphone near the victim's dorm room at the time of the robbery. Colin Zarzecki, Appellant's neighbor, told police that Appellant came to his room the morning of the robbery, "fanned out" a display of cash, and bragged that he had just robbed another student on campus. Appellant told Zarzecki that he and another individual had posed as campus security officers to gain access to the victim's dorm room and had obtained drugs and money out of the victim's footlocker. ***Id***. at 102-105, 124-25.

In addition, when Reilley was interviewed by police, he acknowledged that he knew Appellant from a previous encounter where Appellant had "ripped him off" by taking marijuana from him without payment. N.T., 9/5/18, at 41, 49. We agree with the trial court's assessment that there was sufficient evidence to show Appellant was the one of the perpetrators in the robbery.

In the alternative, Appellant also argues that there was insufficient evidence that he conspired with another individual to commit robbery. We are guided by the following principles:

> To convict a defendant of conspiracy, the trier of fact must find that: (1) the defendant intended to commit or aid in the commission of the criminal act; (2) the defendant entered into an agreement with another (a "co-conspirator") to engage in the crime; and (3) the defendant or one or more of the other co-conspirators committed an overt act in furtherance of the agreed upon crime. 18 Pa.C.S.[A.] § 903. The essence of a criminal conspiracy, which is what distinguishes this crime from accomplice liability, is the agreement made between the co-conspirators.
>
> Mere association with the perpetrators, mere presence at the scene, or mere knowledge of the crime is insufficient to establish that a defendant was part of a conspiratorial agreement to commit the crime. There needs to be some additional proof that the defendant intended to commit the crime along with his co-conspirator. Direct evidence of the defendant's criminal intent or the conspiratorial agreement, however, is rarely available. Consequently, the defendant's intent as well as the agreement is almost always proven through circumstantial evidence, such as by the relations, conduct or circumstances of the parties or overt acts on the part of the co-conspirators. Once the trier of fact finds that there was an agreement and the defendant intentionally entered into the agreement, that defendant may be liable for the overt acts committed in furtherance of the conspiracy regardless of which co-conspirator committed the act.

Commonwealth v. Golphin, 161 A.3d 1009, 1018–19 (Pa.Super. 2017) (citations and quotation marks omitted).

The record in this case contains evidence showing that Appellant planned and executed the robbery with another individual. The conduct of the perpetrators demonstrated they had devised a scheme to commit the robbery as both men wore ski masks to disguise their faces and pretended to be campus police officers to gain access to the dorm room of a student known to sell marijuana. While one man threatened the victim, Reilley, with a firearm, the other perpetrator obtained Reilley's key and stole $1,000 from Reilley's footlocker. The perpetrators also some marijuana from Reilley's desk and then hit both men in the head before escaping the scene. As a result, we agree with the trial court's assessment that there was sufficient evidence to support Appellant's conviction for conspiracy to commit robbery.

Lastly, Appellant contends that his convictions are against the weight of the evidence. Our standard of review is as follows:

> The weight of the evidence is exclusively for the finder of fact who is free to believe all, part, or none of the evidence and to determine the credibility of the witnesses. ***Commonwealth v. Johnson***, 542 Pa. 384, 394, 668 A.2d 97, 101 (1995), *cert. denied*, 519 U.S. 827, 117 S.Ct. 90, 136 L.Ed.2d 46 (1996). An appellate court cannot substitute its judgment for that of the finder of fact. ***Commonwealth v. Pronkoskie***, 498 Pa. 245, 251, 445 A.2d 1203, 1206 (1982). Thus, we may only reverse the lower court's verdict if it is so contrary to the evidence as to shock one's sense of justice. ***Commonwealth v. Hawkins***, 549 Pa. 352, 368, 701 A.2d 492, 500 (1997), *cert. denied*, 523 U.S. 1083, 118 S.Ct. 1535, 140 L.Ed.2d 685 (1998).

> ***Commonwealth v. Small,*** 559 Pa. 423, 741 A.2d 666, 672–73 (1999). Moreover, where the trial court has ruled on the weight claim below, an appellate court's role is not to consider the underlying question of whether the verdict is against the weight of the evidence. Rather, appellate review is limited to whether the trial court palpably abused its discretion in ruling on the weight claim. ***Commonwealth v. Tharp,*** 830 A.2d 519, 528 (Pa.2003) (citations omitted).

Commonwealth v. Champney, 574 Pa. 435, 444, 832 A.2d 403, 408 (2003).

Specifically, Appellant's weight claim is centered on his assertion that the testimony of prosecution witness Colin Zarzecki was not credible. Appellant points out that Zarzecki waited 21 days after the robbery to tell police that Appellant had confessed to the robbery of Reilley's dorm room, only to give conflicting testimony at Appellant's preliminary hearing that Appellant had not told Zarzecki anything about the robbery. After Zarzecki admitted he lied under oath at the preliminary hearing, he was convicted with lying under oath.

At trial, Zarzecki admitted he delayed reporting Appellant's confession as he had reservations about incriminating Appellant, who was his teammate on the Moravian football team. N.T. Trial, 9/5/18, at 100, 109-110. Zarzecki admitted that he lied during his testimony at the preliminary hearing because he was intimidated after seeing other Moravian football teammates had come to support Appellant at the preliminary hearing. ***Id.*** at 112-115. Zarzecki indicated that he became "panicky," "upset," and "extremely nervous" as he

recalled a similar experience when he was younger during which he was threatened by another individual at gunpoint. ***Id***. at 115-118.

While Appellant argues that Zarzecki's testimony was unworthy of belief due his admission of untruthfulness and subsequent conviction of a *crimen falsi* offense for lying under oath at the preliminary hearing, we decline Appellant's invitation to reassess the credibility of the prosecution witnesses and reweigh the evidence at trial. As it was exclusively within the jury's province to weigh these matters, the jury was free to believe Zarzecki's testimony. ***Champney***, ***supra***. As such, we conclude that the trial court did not abuse its discretion in denying Appellant's weight of the evidence claim.

For the foregoing reasons, we affirm.

Judgment of sentence affirmed.

Judgment Entered.

Joseph D. Seletyn, Esq.
Prothonotary

Date: 2/12/20

IN THE COURT OF COMMON PLEAS OF NORTHAMPTON COUNTY
COMMONWEALTH OF PENNSYLVANIA
CRIMINAL DIVISION

COMMONWEALTH OF PENNSYLVANIA, :
: No. C-48-CV-01577-2017
Plaintiff, :
:
v. :
:
ALKIOHN DUNKINS, :
:
Defendant. :

STATEMENT PURSUANT TO PENNSYLVANIA RULE OF APPELLATE PROCEDURE 1925(a)

AND NOW, this 9th day of April 2019, we hereby issue the following statement pursuant to Pa.R.A.P. 1925(a):

On March 19, 2019, Defendant filed timely Notice of Appeal with respect to the judgment of sentence entered in this matter on January 4, 2019, as made final by our Order of Court denying his Post-Sentence Motion on March 1, 2019. On March 22, 2019, we entered an Order directing Defendant to file of record and serve upon the undersigned a statement of the errors complained of on appeal, within 21 days of the date thereof. Defendant timely filed such a statement on April 3, 2019. Therein, Defendant raises six assertions of error, five of which mirror the issues raised by Defendant in his Post-Sentence Motion. Whereas we fully addressed those issues in disposing of Defendant's Post-Sentence Motion on March 1, 2019, we hereby refer to and fully incorporate that Order and Statement of Reasons in response to Defendant's assertions of error in his Statement of Matters Complained of on Appeal. We

"APPENDIX C"

further rely upon the reasoning set forth in support of our Orders of April 26, 2018 and December 7, 2018 disposing of Defendant's Motion to Suppress and Motion for Extraordinary Relief, respectively, to which ¶4 of Defendant's Statement is addressed. No further statement on our part is required with respect to ¶¶1-5 of Defendant's Statement.

However, we find that we must address ¶5(a) of Defendant's Statement, which reads as follows: "Whether the Court erred by refusing to provide Mr. Dunkins with a copy of the notes of testimony for said *in camera* hearing [of October 19, 2018]." The footnote to this paragraph further reads:

> The Court has [o]rdered and explained that it will provide the record of the sealed conference and hearing to the Superior Court but not to undersigned counsel or Mr. Dunkins. Mr. Dunkins is in agreement that the Court providing the notes and record to the Superior Court will be sufficient. However, Mr. Dunkins will be incapable of meeting his burden of ensuring that a full and complete reproduced record is provided to the Superior Court as he has been denied access to the complete record. Additionally, the Commonwealth will be forced to write a response without the record. Equally, without access to the complete record and transcript of the proceedings, Mr. Dunkins will be required to brief this issue relying only on memory and notes of counsel.

In addition to be inconsistent– insofar as Defendant both claims that the Court erred and claims that he "is in agreement" – Defendant's assertion of error and supporting footnote contain misstatements of fact to the extent that he contends that we "refused to provide [him] with a copy of the notes of testimony." Upon receipt of the Defendant's Motion to Unseal, the Court contacted counsel in order to determine the purpose of the request. When counsel indicated that the purpose of the motion was to ensure that the Superior Court would have an opportunity to view the transcript of the *in camera* conference of October 19, 2018, the office of the undersigned communicated with the Northampton County Clerk of Court, Criminal Division

and the Prothonotary of the Superior Court to ensure that the sealed record would be sent to the Superior Court as part of the record on appeal, and that the assigned panel would have the transcript available for review. When this information was relayed by the office of the undersigned to counsel, counsel indicated that he did not require the transcript for another purpose, and that a hearing on the motion would therefore be unnecessary. Same is reflected in the text of our Order of March 20, 2019, wherein we denied the motion because unsealing the record was not necessary to ensure appellate review and unsealing was not requested for any other purpose. For Defendant to suggest now that we refused to unseal the record is disingenuous, as the issue was not reached on the merits as a direct result of counsel's representations.

BY THE COURT:

Paula A Roscioli

PAULA A. ROSCIOLI, J.

IN THE COURT OF COMMON PLEAS OF NORTHAMPTON COUNTY
COMMONWEALTH OF PENNSYLVANIA
CRIMINAL DIVISION

COMMONWEALTH OF PENNSYLVANIA	:	
	:	No. CP-48-CR-01577-2017
v.	:	
	:	
ALKIOHN DUNKINS,	:	
	:	
Defendant.	:	

ORDER OF COURT

AND NOW, this 7th day December 2018, upon consideration of Defendant's Motion for Extraordinary Relief, and following oral argument thereupon, it is hereby **ORDERED** that the motion is **DENIED**, for the reasons discussed below.

STATEMENT OF REASONS

Defendant Alkiohn Dunkins (Defendant) was convicted on September 5, 2018 of robbery, conspiracy to commit robbery, receiving stolen property, and simple assault in connection with an armed robbery that took place on February 2, 2017 in the Hassler dormitory on the campus of Moravian College (Moravian) in Bethlehem, Pennsylvania. Immediately prior to his scheduled sentencing on November 30, 2018, Defendant made an oral Motion for Extraordinary Relief.[1] A written version of the motion was filed on November 26, 2018.

[1] Recognizing that Pa.R.Crim.P. 704(B)(2) indicates that the Court "shall not delay the sentencing proceeding" in order to decide a motion for extraordinary relief, the Court intended to make an oral ruling on the motion and proceed with sentencing on November 30, 2018. However, Defendant requested a continuance of the sentencing in order to make an additional investigation prior thereto. We note that Defendant expressly waived any issue with regard to the timeliness of his sentencing hearing. We note further that the sentencing was originally scheduled for October

"APPENDIX D"

In his Motion for Extraordinary Relief, Defendant asks this Court to vacate his conviction and grant him a new trial. The basis for Defendant's motion is his contention that *Carpenter v. United States*, 585 U.S. ____ (2018), decided June 22, 2018, controls the issue previously decided by this Court in ruling on his Omnibus Pretrial Motion on April 26, 2018. The question raised in Defendant's Omnibus Pretrial Motion – more specifically in a motion to dismiss – was whether law enforcement officers unlawfully obtained records from Moravian College regarding connections to its Wi-Fi network in the absence of a warrant. Finding that Defendant lacked a reasonable expectation of privacy in the records at issue and therefore lacked standing to challenge the warrantless search thereof, we denied his Omnibus Pretrial Motion seeking suppression of that evidence.

In *Carpenter*, the United States Supreme Court considered the question of whether a warrant is required in order for law enforcement to obtain cell site location information (CSLI) from wireless carriers. Briefly, CSLI consists of time-stamped records, maintained by wireless carriers for their business purposes, of a cell phone's connections to "cell sites," which are antennas to and from which connection signals are transmitted for the communication of voice calls, text messages, and other data by cell phones. The cell sites are located at known geographical points, and the locations are recorded in the time-stamped records. When an individual is in possession of a cell phone that is turned on, by virtue of the workings of the phone's constant connection to the nearest cell site and a carrier's collection of CSLI, "he has

---

19, 2019, but was continued at Defendant's request after he obtained new counsel after trial, as new counsel required time to review the record in preparation for sentencing.

effectively been tailed every moment of every day[.]" *Id.* slip op. at 14. Given the realities of modern life and the ubiquity of cell phone use, the collection of CSLI is, essentially, a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 16-17. Holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements *as captured through CSLI*," the *Carpenter* court concluded a warrant is required in order for law enforcement to obtain that information. *Id.* at 11 (emphasis added).

In a similar manner, the Moravian Wi-Fi network consists of over 1,000 connection points located at known geographical points on the Moravian campus, to and from which signals are communicated for the purpose of data transmission, and an analysis of this data enables one to compile of a log of a Wi-Fi network user's historical travels around the Moravian campus as his Wi-Fi enabled device communicated with the various network connection points. In arguing his Motion for Extraordinary Relief, Defendant contends that we must extend the reasoning in *Carpenter* to this case and conclude that, because law enforcement obtained information about Defendant's connections to the Moravian Wi-Fi network without a warrant, the evidence derived therefrom should have suppressed, and that the information of that evidence at trial was erroneous.

At trial, the Commonwealth presented the testimony of Christopher Laird, Director of Systems Engineering at Moravian. Mr. Laird testified that between 1:30 a.m. and 2:30 a.m. on February 2, 2017, during which time two males committed the robbery at issue in the Hassler dorm, devices utilizing three Moravian Wi-Fi accounts were connected to Wi-Fi network

access points in the Hassler dorm. Of those three users, one was a male. That male was Alkiohn Dunkins, Defendant herein. N.T. 9/5/18, pp.218-219. Other data was also obtained from the warrantless search, demonstrating that a device utilizing Defendant's Moravian Wi-Fi user account was connected to various Wi-Fi network access points in and around the Wilhelm and Hassler dorms during the robbery time frame in such a manner demonstrating travel from the Wilhelm dorm, where Defendant lived, to the Hassler dorm and then back to Wilhelm. That evidence was not introduced at trial by the Commonwealth, but was brought out on cross-examination by Defendant's attorney, Phil Viglione, Esq. N.T. 9/5/18, pp.220-225.

While Defendant asks us to conclude that the Moravian Wi-Fi network connection information at issue is identical to CSLI and should be afforded the same protections as those directed in *Carpenter*, we are of the opinion that the Moravian Wi-Fi information is of a materially different character. We are not faced with a circumstance in which the Moravian Wi-Fi network is capable of disclosing the movements of an individual at all hours of the day regardless of where he travels. Quite to the contrary, the network is, by all accounts, confined to the campus of Moravian College. Unlike CSLI, which can monitor the whereabouts of an individual anywhere at any time while in possession of a cell phone – as are most people in the modern age at all times – the Moravian Wi-Fi network is confined to the finite geographic space of a private college campus, similar to a Wi-Fi network that may be made available to patrons shopping in a shopping mall, or a security camera network that may exist at such a mall or at the College. Thus, the historical movements of a Moravian Wi-Fi network user may be gleaned from the network data only insofar as the user was on the campus. We do not

believe that the holding of the *Carpenter* decision was intended to apply to such narrow circumstances. Notably, the *Carpenter* court expressly stated in its decision that it did not "call into question conventional surveillance techniques and tools, such as security cameras." *Carpenter*, supra, at 18.

Also distinguishing CSLI from the Moravian Wi-Fi network is the voluntariness of Defendant's constant connection to the Wi-Fi network. Whereas "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," and therefore, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data," users of the Moravian Wi-Fi network must affirmatively select the option for their Wi-Fi enabled devices to remain connected at all times to the Wi-Fi network for a seamless connection while on the move. *Id.* at 17; N.T. 4/19/18, pp.29, 34; N.T. 9/5/18, p.212. Moreover, as we noted in our April 26, 2018 Order, all users of the Moravian Wi-Fi network must comply with the College's network use policy, which expressly indicates that users cannot and should not have any expectation of privacy with respect to any connections to or data transmitted over the network.

Thus, while the *Carpenter* court held that an individual has an expectation of privacy in his physical movements and that a cell phone user does not voluntarily assume, in a meaningful way, the risk that his physical movements may be discerned by law enforcement obtaining historical CSLI without a warrant, we conclude that a user of the Wi-Fi network at Moravian College who chooses to maintain a constant connection to the network does assume that risk, and, moreover, that his usage of said network is materially different from ordinary

cell phone usage. For this reason, we conclude that *Carpenter* is inapposite here, and that Defendant's Motion for Extraordinary Relief must be denied.

BY THE COURT:

Paula A. Roscioli

PAULA A. ROSCIOLI, J.

IN THE COURT OF COMMON PLEAS OF NORTHAMPTON COUNTY
COMMONWEALTH OF PENNSYLVANIA
CRIMINAL DIVISION

COMMONWEALTH OF PENNSYLVANIA :
: No. CP-48-CR-0157-2017
v. :
:
ALKIOHN DUNKINS, :
:
Defendant. :

ORDER OF COURT

AND NOW, this 26th day of April 2018, upon consideration of Defendant's Omnibus Pretrial Motion, and following a hearing, it is hereby **ORDERED** that Defendant's Motion to Suppress is **DENIED**, for the reasons set forth below. It is further **ORDERED** that Defendant's Motion to Compel Discovery is **GRANTED**, by agreement of the Commonwealth.

STATEMENT OF REASONS

In his Motion to Suppress, Defendant Alkiohn Dunkins challenges a warrantless search and seizure conducted by Moravian College campus police Officer Thomas Appleman of wireless internet connection records maintained by Moravian College.[1] The records at issue reflect the times when and locations where wireless Internet-enabled devices connected to the College's wireless network. Such connections are only made by wireless Internet-enabled devices that are logged in to the College's wireless network using credentials issued to

[1] The actual search of the electronic records was conducted, at the request of Officer Appleman, by Christopher Laird, Director of Systems Engineering at Moravian College.

"APPENDIX E"

students, faculty, and staff of the College.[2] The records of these wireless connections are maintained in the ordinary course of business by Moravian College's information technology department. More specifically, Defendant seeks to suppress the evidence obtained by Officer Appleman indicating that a wireless Internet-enabled device was connected to certain wireless network points on the Moravian College campus in the early morning hours of February 2, 2017 utilizing the username and credentials issued to Defendant as a student at the College.

As a threshold matter, we must first consider whether Defendant herein has standing to challenge the search at issue. To have standing, Defendant must possess a reasonable expectation of privacy in the area searched.

> An expectation of privacy will be found to exist when the individual exhibits an actual or subjective expectation of privacy and that expectation is one that society is prepared to recognize as reasonable. In determining whether a person's expectation of privacy is legitimate or reasonable, the totality of the circumstances must be considered and the determination will ultimately rest upon a balancing of the societal interests involved.

Commonwealth v. Viall, 890 A.2d 419, 422 (Pa. Super. 2005). Importantly, when challenging a warrantless search, it is Defendant who bears the burden of proof to show that he had a reasonable expectation of privacy in the area searched. *Commonwealth v. Enimpah*, 62 A.3d 1028 (Pa. Super. 2013).

At the hearing in this matter, John Conrad, Vice President of Human Resources for Moravian College, testified that all students are required, upon matriculation to Moravian

[2] At a user's discretion, devices can automatically connect to different wireless network connection points as the user moves throughout the College campus, without the need to log in repeatedly, in order to maintain an ongoing wireless Internet connection.

College, to sign an acknowledgement of the Student Handbook wherein numerous College policies, procedures, and regulations are outlined. Students are required to abide by the rules outlined therein. Within the Student Handbook, there is a policy titled "Computing Resources" that provides, in pertinent part:

> Logging in to or otherwise connecting to the campus network implies acceptance of this Moravian College and Moravian Theological Seminary policy.
>
> * * * * * *
>
> The institution's computing equipment and network resources are dedicated to Moravian business to enhance and support the educational mission of Moravian College. These resources include all computers, workstations and multi-user computer systems along with local area networks and wireless networks as well as connections to other computer networks via the Internet.
>
> * * * * * * *
>
> [A]ny data transmitted over institutional assets or connections made through institutional assets are included. The institution has the right to inspect information stored on its system at any time, for any reason, and users cannot and should not have any expectation of privacy with regard to any data, documents, electronic mail messages, or other computer files created or stored on computers within or connected to the institution's network. All Internet data composed, transmitted, or received through the institution's computer system is considered part of the institution's records and, as such, subject at any time to disclosure to institutional officials, law enforcement, or third parties.

Defendant's Exhibit 1, pp.2-3 (emphasis added).

We believe that a plain reading of this "Computing Resources" policy in Moravian College's Student Handbook informs users of the campus wireless network that any connections made to that network are subject to inspection by the College at any time, as well as to disclosure to law enforcement, and that users have no expectation of privacy in that electronic information. Moreover, Defendant offered no additional evidence that would lead us to conclude that he had an expectation of privacy in the records at issue. Thus, we find that

the totality of the circumstances leads us to conclude that Defendant had no reasonable expectation of privacy with respect to the records at issue. See *Commonwealth v. Sodomsky*, 939 A.2d 363, 369 (Pa. Super. 2007) ("If a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents.") citing *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000) (where employee was informed that his internet activity would be scrutinized by employer, he had no legitimate expectation of privacy in his internet activity); *United States v. King*, 2006 WL 3421253 (M.D.Ala. 2006) (defendant knowingly exposed personal files to public by linking to network after being informed that personal files could and would be searched even though he attempted to protect files from search); *Lown v. State*, 172 S.W.3d 753 (Tex. App. 2005) (defendant did not have reasonable expectation of privacy in files on work computer which were backed up at request of people in authority at defendant's company). Accordingly, we find that Defendant's Motion to Suppress must fail.

BY THE COURT:

Paula A. Roscioli

PAULA A. ROSCIOLI, J.