[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.

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.

---

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.