[J-3-2021] [MO: Dougherty, J.]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

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

CONCURRING AND DISSENTING OPINION

JUSTICE WECHT **DECIDED: November 17, 2021**

I.

In *Carpenter v. United States*,[1] the Supreme Court of the United States held that, because "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" cell-site location information ("CSLI"),[2] the

---

[1] ___ U.S. ___, 138 S. Ct. 2206 (2018).

[2] *Carpenter*, 138 S. Ct. at 2217. In *Carpenter*, the Supreme Court described how CSLI records are generated:

> 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 [CSLI].

Id. at 2211.

retrieval and examination of such records constitutes a search for Fourth Amendment purposes. We took this case 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. To the hundreds of post-secondary institutions in Pennsylvania and to the thousands upon thousands of students that are enrolled in those institutions, guidance and clarity in this area of law is critical.

Each academic year, more and more post-secondary schools are mandating use of the internet to satisfy at least part of the curriculum. Most, if not all, of these colleges and universities already have a campus-wide Wi-Fi network. Those that do not almost certainly will do so soon. It is safe to say that virtually every college student carries at least one internet capable device everywhere he or she goes on campus. Logging onto the school's Wi-Fi is not without consequence. Before students may connect their devices to school Wi-Fi networks, they often must sign an agreement consenting to various limitations on their use of the networks and, as is the case here, waiving any expectation of privacy that students have in any records created through use of the network.

The confluence of these circumstances at modern post-secondary institutions raises questions that this Court has yet to answer. For example, we have not considered whether compulsory waivers of the kind imposed upon college students are enforceable, particularly when information obtained as a result of such waivers is offered as evidence in criminal cases. In the event that such waivers facially are binding, we have not had occasion to articulate what language or conditions must be contained within them to ensure that the student giving up his or her constitutional rights is making a knowing, intelligent, and voluntary choice. Is such a volitional act possible when the student is

compelled to sign a waiver as a condition of admission to or attendance at a college or university?

But those (and similar) questions are secondary. There is no need to explore the propriety and requirements of a full-scale waiver of one's right if no such right exists in the first place. One cannot waive what one does not possess. The threshold question is whether, in the wake of *Carpenter*, students retain an expectation of privacy in the records created when their internet-capable devices connect to campus-wide Wi-Fi networks. The answer is the keystone to every other subsequent legal question. If students have no such expectation of privacy, there is no reason to inquire into the validity of any waivers, and universities and colleges freely can seek, or forego, them.

Instead of answering this important constitutional question, the Majority skips to the end of the analysis and holds only that, under the factual circumstances of this particular case, and without citation to precedents addressing the enforceability of similar blanket waivers, Alkiohn Dunkins abandoned any rights that he may have had.[3] The decision resolves only this appeal, has virtually no precedential value, and provides no guidance to colleges and universities, students, or bench and bar. Pennsylvania's post-secondary institutions must continue to create handbooks and seek waivers in the constitutional dark, not having received from this Court even the most elementary discussion of the existence (or non-existence) of limits on what they can ask of incoming pupils. Students have no choice but to yield to the policies, without knowing whether they are required to do so as a matter of constitutional law. Those who have a meaningful interest in these issues are no better informed today than they were before we took this case. The Majority could have achieved as much by dismissing this appeal as improvidently granted.

---

[3] *See* Maj. Op. at 10.

This is not to say that the Majority's decision to sidestep the critical issue here is unreasonable or without legal support. In limiting its review and resolution of this case, the Majority relies upon the well-established precept of judicial restraint that "courts should avoid constitutional issues when the issue at hand may be decided upon other grounds." *Id.* at 7 n.5 (quoting *In re Fiori*, 673 A.2d 905, 909 (Pa. 1996)). I agree that this self-imposed limitation is a "sound tenet of jurisprudence." *Id.* But it is not an inflexible, inexorable, exception-free command. The Majority's own formulation of the principle, using the word "should," highlights the reality that there are instances in which the principle must yield. "Should" does not mean "shall." To my knowledge, we have never suggested that the principle applies without exception. We generally speak of constitutional avoidance in terms that admit of some flexibility. *See In re Stevenson*, 12 A.3d 273, 275 (Pa. 2010) ("[A]s a general matter, **it is better** to avoid constitutional questions if a non-constitutional ground for decision is available.") (emphasis added). To find a circumstance in which the principle of constitutional avoidance should not apply is not to "abandon" it,[4] but rather to recognize that generally sound principles must occasionally yield to pressing jurisprudential demands.

The case before us is one in which addressing, at least in part, the constitutional question is warranted. With today's technology, records created by constant and automatic connections to Wi-Fi networks can create a highly accurate documentary history of a student's movements every moment of every day that he or she is on campus. The collection of these records implicates serious and important privacy concerns. Bypassing this inquiry achieves little in this complicated area of law and leaves too many interested parties (and their rights to collect the data or to avoid collection of the data) in

[4] *See* Maj. Op. at 7 n.5.

the lurch. It is important to these institutions and to students that this Court offer as much guidance as the circumstances of this case allow. I would do so here.

Upon doing so, it becomes clear that the circumstances of this case differ substantively from those that drove the Supreme Court's ruling in *Carpenter*. Unlike the cell phone user in *Carpenter*, the Moravian College student in this case has the reasonable ability to control and limit the creation of the Wi-Fi records. Consequently, I would find *Carpenter* to be distinguishable, and would hold that a student who voluntarily chooses to automatically—and at all times—connect to a campus Wi-Fi network does not have an expectation of privacy in the records created from that decision. This case would be entirely different if the college provided no opt-out mechanism, essentially locking the students into the network and affording them no reasonable opportunity to prevent the creation of the historical records. Under such circumstances, it would be more likely that the student would retain an expectation of privacy. But that is not what happened here, and, accordingly, Dunkins retained no such expectation of privacy. For this reason, I concur in the result reached by the Majority.

II.

Moravian is a private liberal arts college located in Bethlehem, Northampton County. Like most schools, Moravian has had to adapt and modernize both its infrastructure and its educational operations to account for the ever-increasing role that the internet plays in people's lives. At Moravian, access to the internet has developed over time from a useful, but not essential, tool into an integral and indispensable aspect of the educational experience, so much so that internet access, including Wi-Fi, is a requirement for portions of Moravian's academic curriculum. Indeed, by the 2016-2017

academic year, widespread and constant internet access was an essential component of a Moravian student's social and educational life.

To accommodate this new reality, Moravian sought to provide its students with "curb-to-curb wireless" internet service.[5] The college created a network that offered authorized users wireless internet access at any physical location on campus, including classrooms, residence halls, athletic fields, and the outdoor areas adjacent to the campus' physical buildings. To ensure that the vast network provided reliable and constant internet connectivity, Moravian installed around its campus approximately 1,300 Wi-Fi access points, which connect seamlessly to a user's devices and permit access to the network.

Each Moravian student is provided with a username and a randomly generated password. When a student attempts for the first time to access Moravian's Wi-Fi network on an internet-capable device (such as a smartphone or laptop), the student is prompted to enter his or her username and password. The student also is given the option to select a feature that connects the student to the network automatically. Students who choose to make this selection are not required to input usernames or passwords every time they connect to the network or to different Wi-Fi access points.

As a student moves around campus while connected to Moravian's network, the student's device connects automatically to the nearest access point or the access point that provides the strongest signal. Each time this happens, a record is generated that identifies the access point to which the user has connected, the unique log-in information of the user that accessed that point, and the time that the connection occurred. Much like the records created when smartphones connect with cellular towers as in *Carpenter*, the access point records created by Moravian's Wi-Fi network can provide a rather accurate

---

[5] Notes of Testimony ("N.T."), 9/5/2018, at 208.

recreation of a student's movements around campus, along with a general timeline of those movements.

Each enrolling student at Moravian is provided with a lengthy student handbook which explains the various policies that govern many aspects of student life at Moravian. In the handbook, students are advised to read and become familiar with the college's policies. Before students can officially begin college at Moravian, they must complete an electronic form acknowledging the receipt of the handbook and consenting to its terms and conditions. This includes consenting to the terms and conditions that are set forth in the handbook's "Computing Resources" policy, which provides, in pertinent part, as follows:

> 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**.

Suppression Ct. Op., 4/26/2018, at 3 (citing Def.'s Ex. 1, at pp. 2-3) (emphasis provided by suppression court).

Moravian's extensive Wi-Fi network and its corresponding "Computing Resources" policy both were in place during the 2016-2017 academic year, when William Reilley enrolled as a freshman. Reilley shared a dormitory room with fellow student Greg Farina. Soon after starting his freshman year, Reilley began selling marijuana. Reilley soon learned that drug dealing is an occupation that can spiral out of control and land a person in unpredictable (and sometimes perilous) situations. One such situation occurred in January 2017 when Reilley tried to sell marijuana to the appellant in this case, Dunkins. Dunkins, a fellow Moravian student at the time, contacted Reilley in mid-January and arranged a transaction. Reilley agreed to meet Dunkins in a college restroom located on the Moravian campus. Once there, Reilley entered an empty stall; Dunkins was in the adjoining stall. Reilley slid the agreed-upon amount of marijuana under the shared stall wall. Dunkins did not uphold his end of the bargain. Instead, Dunkins took the marijuana and walked out of the restroom without paying. Because of the illegal nature of the transaction, Reilley did not call the police to report the theft.

A few weeks later, on February 2, 2017, Reilley returned to his dorm room at around 1:30 a.m., ate a snack, and went to bed. At around 2:00 a.m., Reilley heard a knock on the door. Believing the visitor might be a campus security officer, Reilley instructed Farina to open the door. When Farina did so, two men wearing black ski-masks, dark t-shirts, and khaki pants burst in. The first man to enter —the shorter of the two—immediately punched Farina in the face, knocking him back from the doorway. The second man walked further into the room and pointed a 9 millimeter handgun at Reilley, who was still lying down. Reilley jumped out of bed and raised his hands in the air. The gunman scanned the room until his eyes landed upon a locked footlocker. The gunman

demanded the locker key. Reilley retrieved the key from a pants pocket and handed it over. The gunman handed the key to his shorter companion, who opened the locker and found approximately $1,000 in cash. The shorter man then rifled through Reilley's desk drawers and found a jar of marijuana. The two masked men took the money and the marijuana and headed toward the door. Before leaving, the gunman punched Reilley on the side of the head and then walked over to Farina and punched him as well. The two masked men then fled.

Based upon his recent experience with Dunkins in the college restroom, Reilley believed that Dunkins was one of the two robbers. Reilley assumed that Dunkins suspected Reilley had more marijuana in his dorm room and decided to rob him, having suffered no consequences from the first incident. Nonetheless, Reilley initially did not contact school or law enforcement authorities to report the robbery, even though Farina wanted to do so. Reilley was apprehensive over his own criminal exposure and was not yet ready to involve the police.

Reilley went to work the next day, albeit an hour or two late. While there, Reilley remained emotionally shaken from the robbery, which had occurred around nine hours earlier. Reilley decided to report the night's events to the school counselor, who promptly took Reilley to the campus police to file an official report. Reilley reported the armed robbery to Officer Thomas Appleman of the Moravian Campus Police Department. Officer Appleman directed another officer to secure the dorm room, and then contacted the City of Bethlehem Police Department for assistance in conducting a forensic examination of that room. Personnel from the two police departments worked together to process the scene and investigate the crime.

To help identify the perpetrators of the robbery, Officer Appleman asked Moravian's director of systems engineering, Christopher Laird, to review the Wi-Fi records

from the relevant night in question in an effort to ascertain whether a student had connected to the access points near Reilley's dormitory around the time of the robbery. Upon review of those records, Laird determined that only three people who did not reside in the building had connected to the Wi-Fi network around that time. Two of those people were women, and thus were excluded as suspects. The third person was Dunkins. As a Moravian student, Dunkins voluntarily had signed the student handbook and thus had consented to the "Computing Resources" policy that permitted Laird to retrieve the data without a search warrant and without seeking Dunkins' prior approval. Laird reported this finding to Officer Appleman, who, in turn, relayed it to Detective James Ruvolo of the City of Bethlehem Police Department, who by that point had assumed control of the investigation.

Detective Ruvolo discussed Laird's findings with Reilley. Upon learning that Dunkins was a suspect, Reilley reported to Detective Ruvolo that this was not the first time that Dunkins had taken marijuana from him. Reilley then reported the earlier bathroom stall incident to the detective.

When later questioned by police, Dunkins claimed not to have been in Reilley's dormitory building on February 2, 2017, and denied any involvement in the robbery. However, as the investigation continued, the evidence against Dunkins continued to mount. For instance, the police interviewed Dunkins' dormitory neighbor, Colin Zarzecki, who told the officers that, the night after the robbery, Dunkins came to Zarzecki's dorm room and showed off a large amount of cash. According to Zarzecki, Dunkins stated that he had acquired the money in a recent robbery. Dunkins then told Zarzecki that he and another person posed as campus security officers in order to gain access to the victims' dorm room. Once inside, Dunkins boasted, the two stole money and drugs from a footlocker.

Dunkins was arrested and charged with robbery, conspiracy to commit robbery, receiving stolen property, and simple assault.[6] Prior to trial, Dunkins filed a suppression motion, in which he contended that the police had violated his Fourth Amendment rights by seizing and searching Moravian's Wi-Fi records without first obtaining a search warrant. On April 26, 2018, after hearing two days of testimony, the trial court denied Dunkins' motion. In a statement accompanying its order, the trial court opined that Dunkins could not challenge the seizure of the Wi-Fi records, including those that placed him in Reilley's dormitory building at the time of the robbery, because Dunkins lacked an expectation of privacy in those records. The court relied in substantial part upon Dunkins' assent by signature to the "Computing Resources" policy. The court explained that the policy "informs users of the campus wireless network that any connections made to that network are subject to inspection by [Moravian officials] at any time, as well as to disclosure to law enforcement, and that users have no expectation of privacy in that electronic information." Suppression Ct. Op., 4/26/2018, at 3. Thus, based upon the totality of the circumstances, and lacking any evidence to the contrary, the trial court found that Dunkins had no expectation of privacy in the records and that his suppression motion "must fail." *Id.* at 4. Notably, at the time of the trial court's ruling, *Carpenter* had not yet been decided.

Following a two-day jury trial, Dunkins was convicted on all charges. On November 21, 2018, Dunkins filed a post-trial motion for extraordinary relief. When the parties appeared for sentencing on November 30, 2018, Dunkins reasserted his claim for extraordinary relief, this time orally in open court. Dunkins sought reconsideration of the denial of his suppression motion based upon the Supreme Court's intervening recognition

---

[6] 18 Pa.C.S. §§ 3701(a)(1)(ii), 903, 3925(a), and 2701(a)(1), respectively.

of a person's expectation of privacy in cellular tower records in *Carpenter*, which had been decided a few months earlier.

By written order dated December 7, 2018, the trial court denied relief. In its accompanying statement, the trial court first summarized *Carpenter*. In doing so, the court highlighted the Supreme Court's finding that, due to the geographical pervasiveness of cellular towers and the inseparable relationship between a modern person and his or her smartphone, CSLI records effectively permit the person to be "tailed every moment of every day[.]" Trial Ct. Op., 12/7/2018, at 3 (quoting *Carpenter*, 138 S. Ct. at 2218). The court emphasized the Supreme Court's ruling that, because of this susceptibility to extensive tracking, a person has an expectation of privacy in records "'*as captured through CSLI*.'" *Id.* (quoting *Carpenter*, 138 S. Ct. at 2217) (emphasis added by trial court).

The trial court then turned to Dunkins' argument that Moravian's Wi-Fi network, with its 1,300 access points and its corresponding ability to track a student's movements across the campus using the records created by those access points, was sufficiently akin to the cellular towers at issue in *Carpenter* such that the same expectation of privacy existed for users of the Wi-Fi network. The court rejected this comparison, finding instead that the Wi-Fi network and the cellular towers were of "a materially different character" from one another:

> 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 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.

Id. at 4. Noting that the *Carpenter* Court expressly declined to "'call into question conventional surveillance techniques and tools, such as security cameras,'" the trial court concluded that *Carpenter*'s expectation-of-privacy ruling should not be extended beyond "such narrow circumstances." *Id.* at 5 (quoting *Carpenter*, 138 S. Ct. at 2220).

In addition to the differences in geographical parameters, the trial court discerned another material distinction between connections to cellular towers and Wi-Fi networks: voluntariness. In *Carpenter*, the Supreme Court noted that mobile phones, which have become an indispensable necessity in contemporary life, connect automatically to cell towers merely by being powered on. The only way to prevent the connections, and, derivatively, the generation of records, is to turn the device off and disconnect from the network. By contrast, connection to Moravian's Wi-Fi network is voluntary; a student must choose affirmatively to connect automatically to the access points as he or she moves around campus. Alternatively, the student may choose to log on only when he or she wishes to do so, thereby generating records only when the student allows them to be created. By opting into the automatic connection aspect of the Wi-Fi network, the trial court opined, the student "does assume the risk" that records will be created and later seized by law enforcement. *Id.* at 5. The "Computing Resources" policy expressly informed the student of this possibility associated with use of the network.

The trial court sentenced Dunkins to an aggregate term of five to ten years' imprisonment. Dunkins then filed post-sentence motions, which the trial court denied. Thereafter, Dunkins filed a notice of appeal and a Pa.R.A.P. 1925(b) concise statement of errors complained of on appeal. The trial court then issued a Rule 1925(a) opinion incorporating its prior orders and its statements in response to the issues that Dunkins raised in his Rule 1925(b) statement.

In the Superior Court, Dunkins argued, as he had in the trial court, that *Carpenter*'s expectation of privacy ruling extended to the records created by Moravian's Wi-Fi network. *Commonwealth v. Dunkins*, 229 A.3d 622, 625, 628 (Pa. Super. 2020). The Superior Court disagreed, and affirmed the trial court. *Id.* at 625, 634. After summarizing the key aspects of the case, the panel emphasized that the *Carpenter* Court had described its ruling as "narrow." *Id.* at 629 (quoting *Carpenter*, 138 S. Ct. at 2220). The *Carpenter* Court had noted that its decision should not be read to question "conventional surveillance techniques and tools, such as security cameras . . . or business records that might incidentally reveal location information." *Id.* (quoting *Carpenter*, 138 S. Ct. at 2220). Particularly relevant to the panel's analysis, the Supreme Court had confined its *Carpenter* ruling to CSLI records as they were obtained in that case—requests for all data related to a particular, known telephone number—and deliberately had expressed no view on how, or whether, its decision would apply to accessing records and information using what are known as "tower dumps." *Id.* This latter method of data collection differs from the method used in *Carpenter* in that, instead of requesting all records created by a known telephone number as it connects to any number of towers, a "tower dump" focuses upon a single tower and provides a requesting party with the data related to every telephone that connects to that particular tower during a prescribed period. *See Carpenter*, 138 S. Ct. at 2220 (defining a "tower dump" as "a download of information on all the devices that connected to a particular cell site during a particular interval")[7]

According to the Superior Court, the express exemption of "tower dumps" from *Carpenter*'s holding was fatal to Dunkins' argument for *Carpenter*'s applicability. This

[7] *See also United States v. Pembrook*, 876 F.3d 812, 816 (6th Cir. 2017) (*reversed on other grounds* by multiple Supreme Court cases and orders) (describing a "tower dump" as "a chronological list of every phone number that used the tower for any purpose (voice call, text, internet connection, etc.) regardless of provider (e.g., Verizon, AT&T)").

was because, the court determined, when the campus police sought the Wi-Fi records for the access point in Reilley's dormitory building on the night of the robbery, the request was "akin to a 'tower dump.'" *Dunkins*, 229 A.3d at 629. "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 Wi-Fi in [Reilley's] dorm at the time of the robbery." *Id.* Consequently, the panel concluded that *Carpenter*, by its own limiting terms, did not apply to the circumstances of this case.

The Superior Court discerned additional reasons for rejecting Dunkins' suppression arguments. First, the court agreed with the trial court that a cellular network created by cellular towers differs materially from a college-wide Wi-Fi network. For one thing, the panel explained, records generated by accessing cellular towers can track and record an individual's movements at all times of the day, regardless of where that person goes. A Wi-Fi network, on the other hand, collects only data that is generated when a person logs on to that network, and is limited to that person's movements within the smaller, limited geographical boundaries of the campus. *Id.* Unlike cellular phones, which are inseparable from their users in modern society and connect automatically to towers so long as the device is turned on, use of a Wi-Fi network is optional. A student can choose to log off at any time and thereby prevent creation of any records of his or her movements. Thus, the Superior Court viewed the gathering of data from a Wi-Fi access point voluntarily accessed as no different from information obtained from a security camera posted outside the door of a dormitory building. *Id. Carpenter* does not recognize an expectation of privacy in data collected by security cameras.

Second, regardless of the merits of any *Carpenter*-based argument, the Superior Court deemed Dunkins' overall argument for suppression to be unreasonable, because 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" to law enforcement. *Id.* at 630. Relying upon its own decision in *Commonwealth v. Sodomsky*, 939 A.2d 363 (Pa. Super. 2007), the Superior Court stressed that, when a person freely provides a third party with access to the contents of his or her computer, that person abandons any expectation of privacy in the exposed material. *Dunkins*, 229 A.3d at 630 (quoting *Sodomsky*, 939 A.2d at 369). For further support of its enforcement of Dunkins' waiver of his expectation of privacy when using the network, the court turned to decisions from other jurisdictions, most notably the United States Court of Appeals for the Seventh Circuit. In *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019), that federal court held that a "defendant can voluntarily consent in advance to a search as a condition of receiving contracted services." *Dunkins*, 229 A.3d at 630 (quoting *Adkinson*, 916 F.3d at 610; and discussing *Medlock v. Trs. of Indiana Univ.*, 738 F.3d 867 (7th Cir. 2013)). Accordingly, the plain language of Moravian's policy, and Dunkins' knowing, intelligent, and voluntary acquiescence in that policy, resulted in a clear waiver of any expectation of privacy that Dunkins had in the records generated by the Wi-Fi network's access points. *Id.* at 631. The Superior Court highlighted that Dunkins could have chosen to use a wireless carrier's internet service, or he could have selectively signed on and off of the network in order to avoid creating a data trail. Because Dunkins selected the option to connect automatically to the Moravian network as he roamed the campus, he was bound by the terms of the policy to which he agreed, meaning that he had no expectation of privacy in the material and could not later complain about the use of that information against him. *Id.*

This Court granted allowance of appeal in order to address the following issue:

> Whether the trial court erred by denying Mr. Dunkins' 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*).

Dunkins' primary contention here is that *Carpenter* compels, at a minimum, an equivalent finding that, for Fourth Amendment purposes, a person can assert a reasonable expectation of privacy in records that are created when that person's device connects automatically to the various access points of an extensive Wi-Fi network. Dunkins goes one step further and maintains that the privacy interest in Wi-Fi records is even greater than that recognized in the CSLI records in *Carpenter*, for two reasons. First, Dunkins contends, Wi-Fi records can establish a person's location with more precision than can CSLI records. Second, unlike CSLI records, which generally only indicate that a person passed through a general geographical area at a certain time, Wi-Fi records can track a person's movements even after the person enters a building, including residences, thereby implicating far weightier privacy interests. Accordingly, Dunkins argues, the lower courts erred in holding that *Carpenter* does not apply here.

In order properly to weigh Dunkins' arguments, it is necessary to begin with a review of *Carpenter*. In 2011, police officers arrested four men for committing a string of robberies at various electronics stores throughout Michigan and Ohio. *Carpenter*, 138 S. Ct. at 2212. It turned out that the four arrestees were part of a larger criminal organization that had been perpetrating similar robberies over the previous four months. While confessing to these offenses, one of the men identified a slew of other participants in the crime spree and provided cellular telephone numbers for those individuals to the FBI. One of the additional suspects that was identified during the suspect's confession was Timothy Carpenter. Prosecutors sought, and obtained, two court orders under the Stored Communications Act to retrieve CSLI records related to Carpenter's cellular device over the four-month period during which the robberies occurred. Notably, under the Stored

Communications Act, prosecutors could obtain the relevant records merely by presenting "specific and articulable facts showing that there are reasonable grounds to believe" that the records were "relevant and material to an ongoing criminal investigation."[8] Execution of the two orders resulted in the production of approximately 130 days of Carpenter's phone records. From that data, prosecutors and law enforcement agents obtained almost 13,000 geographical points—over 100 points per day—that enabled them to identify Carpenter's location and to reconstruct his movements during those four months. *Id.*

Carpenter was arrested and charged with crimes related to the series of robberies. Prior to trial, he filed a motion to suppress the CSLI records, arguing that obtaining such records constituted a search that required a showing of probable cause, not the lesser standard of "reasonable grounds." The District Court denied the motion. At trial, the CSLI records were introduced to the jury along with expert testimony. The prosecutor used the records to establish that Carpenter was in the precise areas at the exact times that the robberies occurred. He was convicted and sentenced to over 100 years in prison.

The Supreme Court granted *certiorari* in order to determine "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Id.* at 2211. To constitute a search for constitutional purposes, state actors must intrude upon the privacy rights of an individual either by obtaining information by trespass upon the physical property owned by the individual or by otherwise intruding upon an area in which the individual has a reasonable expectation of privacy. *Id.* at 2213 (citations omitted). When the asserted expectation of privacy is "one that society is prepared to recognize as reasonable," government officials first must obtain a search warrant supported by probable cause before they may conduct a search. *Id.* (quoting *Smith v.*

---

[8] 18 U.S.C. § 2703(d).

Maryland, 442 U.S. 735, 740 (1979)). The question for the Court thus became whether a person has an expectation of privacy in the CSLI records; if so, retrieval of such records under the Stored Communications Act's lesser "reasonable grounds" standard would be unconstitutional.

The Court observed that the collection of cell-site records is not a law enforcement act that readily can be assessed using the Court's existing precedents. Rather, "requests for cell-site records lie at the intersection of two lines of cases." *Id.* at 2214. The first line of cases addresses whether a person has an expectation of privacy in his physical location or movements in public. In these cases, the Court long has held that, in general, a person cannot invoke any such expectation of privacy. *Id.* at 2215 (quoting *United States v. Knotts*, 460 U.S. 276, 281 (1983)). Any such expectation would be unreasonable, given that, by openly moving about in public, a person voluntarily displays his movements to anyone who cares to look. *Id.* This general rule is not absolute. Different principles necessarily apply when law enforcement goes beyond general observations of a person's public movements and instead conducts more extensive surveillance. Thus, in *United States v. Jones*, 565 U.S. 400 (2012), the Court recognized a person's expectation of privacy in the records of his movement that were obtained using a GPS device installed on a vehicle. Of critical import in *Jones* was the resulting ability of law enforcement officers to track a person's every movement over a period of time. *Carpenter*, 138 S. Ct. at 2215 (quoting *Jones*, 565 U.S. at 430).

The second set of decisions that the *Carpenter* Court identified as relevant implicates the third-party doctrine. The Court's leading third-party doctrine cases, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, *supra*, stand generally for the proposition that a person retains no expectation of privacy in information that he or she voluntarily discloses to another person. Once a person conveys that information to

someone else, he or she "assumes the risk" that the information later will be turned over to law enforcement. *Smith*, 442 U.S. at 745.

The Court queried whether these Fourth Amendment cases applied to this "new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." *Carpenter*, 138 S. Ct. at 2216. On the one hand, the Court found categorical similarities between the collection of data from cellular towers and from the GPS device in *Jones*, indicating at least facial applicability of the reasoning from *Jones*. The Court explained that both categories of data are "detailed, encyclopedic, and effortlessly compiled." *Id.*

By contrast, the Court determined that the third-party doctrine had little, if any, usefulness in these circumstances. The Court noted that, while the doctrine, born in the late 1970s, logically applies to things like bank records and telephone numbers, "it is not clear whether its logic extends to the qualitatively different category of cell-site records." *Id.* at 2216-17. The Court continued, "[a]fter all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 2217.

The Court rejected the view, advanced by the Government and by Justice Kennedy in dissent, that CSLI data should be treated as business records and, as such, subject to the third-party doctrine. This perspective failed "to contend with the seismic shifts in digital technology" that permit an all-encompassing compilation of a person's public movements "for years and years." *Id.* at 2219. "There is a world of difference between the limited types of information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* Invocation of the

third-party doctrine would not reflect a "straightforward application," but would instead mark a "significant extension of it to a distinct category of information." *Id.*

The Court emphasized that the third-party doctrine is predicated upon a reduced, but not non-existent, expectation of privacy in information knowingly shared with another. That a privacy interest is diminished does not mean that the Fourth Amendment "falls out of the picture entirely." *Id.* at 2219 (quoting *Riley v. California*, 573 U.S. 373, 392 (2014)). The third-party doctrine requires contemplation of both the act of sharing and the type of information shared to determine whether an expectation of privacy exists in the contents of that information. With regard to the tower records, the Court found "no comparable limitations on the revealing nature of CSLI," and, thus, rejected a mechanical application of the doctrine. The case was "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 2220.

Nor did the doctrine apply mechanically simply because a cell phone user voluntarily allowed the data to be created. "Cell phone location information is not truly 'shared' as one normally understands the term." *Id.*

> In the first place, 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. *Riley*, 573 U.S. at 385. Second, 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. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[] the risk" of turning over a comprehensive dossier of his physical movements." *Smith*, 442 U.S. at 745.

Id.

Thus, the Court concluded, the third-party doctrine simply did not operate to preclude an expectation of privacy in this type of records. The Court therefore held that, "[g]iven the unique nature of cell phone location records," regardless of "[w]hether the government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier," a person "maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217. It follows that the act of obtaining location information from a wireless carrier is a search for purposes of the Fourth Amendment, *id.* at 2217, 2220, and that, before law enforcement officers can perform that search, they must get a search warrant. *Id.* at 2221. The Court then explained that orders issued under the Stored Communications Act were constitutionally deficient because the statute requires only a showing of "reasonable grounds," a standard that "falls well short of the probable cause requirement for a warrant." *Id.*

The Court construed its decision as "a narrow one," its reach limited to the type of data collected (and to the method of collecting that data) in the case. *Id.* at 2220. The Court declined to address other, albeit related, methods of data collection, such as real-time CSLI or "tower dumps." The Court similarly noted that its decision should not be read to disturb the traditional application of the third-party doctrine nor extended to circumstances involving other types of business records that might reveal a person's geographical location at a given time. Finally, the Court cautioned that the decision did not "call into question" other types of surveillance tools, such as security cameras. *Id.*

The central issue in the case before us today is whether the expectation of privacy recognized and deemed reasonable by the Supreme Court in *Carpenter*—a case involving a vast, widespread network of cellular towers—applies to an extensive, but more geographically limited, campus-wide Wi-Fi network. Both the trial court and the Superior

Court concluded that, because the differences between these two networks were material and substantive, *Carpenter* did not apply. In particular, both of the lower courts concluded that, because the Wi-Fi network at Moravian is confined to the boundaries of the college's campus, and is not as geographically expansive as a cellular network, the Wi-Fi network operates more like networks established at a shopping mall or like a system of security cameras.

I find these comparisons unpersuasive. Ultimately, I agree with our lower courts that there exists no expectation of privacy in the records created in this case, but my reasoning differs.

At the heart of the Supreme Court's analysis in *Carpenter* was the inextricable relationship that has developed in modern society between a person and his or her internet-capable device. It is hardly debatable that the use of mobile devices is "indispensable to participation in modern society." *Id.* at 2220 (citing *Riley*, 573 U.S. at 385). The modern use of the internet in many ways parallels cell phone usage. Cell phones, smart devices, and computers have evolved in a way that integrates the internet into nearly every aspect of their operation and function. Advancements in the ability to use the internet have turned communication technologies that once were futuristic and fantastical gadgets possible only in the world of the Jetsons or Dick Tracey into everyday realities. Physical distance is no longer a barrier to face-to-face interaction. Applications such as Zoom, WebEx, and Skype allow face-to-face, personal, professional, and educational discussions that previously could be performed only in person or by conference call or telephone call. We now have at our fingertips the ability to manage our calendars or access an unlimited amount of information, regardless of where we are located. Instantaneously, a person can check news reports, weather forecasts, sports scores, and stock prices. Modern matchmaking and dating commonly now begin with

internet connections. As time passes, the internet has come to be used and relied upon in nearly every aspect of our daily lives, from organizing family reunions, to scheduling medical appointments, to conducting academic research, to operating every aspect of a business.

Colleges and universities have not stood apart as this technological evolution has accelerated. Where students once carried pens and notebooks, they now carry internet-connected laptops and tablets. In the past, students stored their documents in folders and portfolios; now, much of a student's work is stored in the "cloud."[9] Professors use internet-based programs to communicate with students, to post syllabi and course materials, and to administer exams.[10] Course texts and lab manuals often are available only online. Things have progressed far enough that the internet is not used only to *facilitate* the educational experience. For some colleges and universities, the internet *is* the entire educational experience, allowing students to earn college degrees from the comfort of their own homes.[11] At Moravian, having a connection to, and use of, the internet has become a mandatory aspect of the academic curriculum.[12]

---

[9] "Simply put, the cloud is the Internet—more specifically, it's all of the things you can access remotely over the Internet. When something is in the cloud, it means it's stored on Internet servers instead of your computer's hard drive." *What is the cloud?*, GCFGLOBAL, https://edu.gcfglobal.org/en/computerbasics/understanding-the-cloud/1/ (last visited July 7, 2021).

[10] One popular example of an internet-based educational management program is Blackboard Learn, which is a "[w]eb-based server software" that provides a "virtual learning environment and learning management system." Blackboard Learn "features course management, customizable open architecture, and scalable design that allows integration with student information systems and authentication protocols." *Blackboard Learn*, WIKIPEDIA.ORG, https://en.wikipedia.org/wiki/Blackboard_Learn (last visited July 7, 2021).

[11] For example, the University of Phoenix is an exclusively online program. UNIVERSITY OF PHOENIX, www.phoenix.edu (last visited July 7, 2021).

[12] N.T., 9/5/2018, at 207.

However, the mere prevalence of the internet in the daily life of a college student does not automatically mean that *Carpenter* applies to the records in the case. *Carpenter's* expectation of privacy ruling was based upon more than just the fact that a contemporary American and his or her phone rarely, if ever, detach from one another. Nor was the decision premised exclusively upon the widespread coverage provided by cellular towers, or upon the fact that the records generated from connections to those towers can create an all-encompassing roadmap of the person's movements. The ruling resulted from the amalgamation of these factors. Indeed, the linchpin of *Carpenter* was that, because of the inseparable relationship between a person and his cell phone, it is not objectively reasonable to expect that a cell phone user can avoid the creation of the records as he or she travels through the public sphere. Because the user has no reasonable way to limit the creation of the records, and because of the extensive information compiled by those records, the Court found that a reasonable expectation of privacy existed. The inverse must also be true: if a person can limit the creation of the records, or if the device or instrumentality at issue is not so inextricably and unavoidably attached to modern life, no such expectation of privacy would prevail.

The question here is whether the same considerations that led the *Carpenter* Court to its expectation of privacy ruling are present with regard to one who accesses the internet via a particular Wi-Fi network. The answer, at least under the facts of this case, is "no." The primary difference between the use of cell phones and the use of the internet is that a person simply can choose not to connect to a particular Wi-Fi network, or can choose to log off of the internet at any time. This was something that the *Carpenter* Court deemed impractical, if not entirely impossible, in today's society with regard to cell phones. This also is why the Superior Court in this case compared Moravian's Wi-Fi network to a Wi-Fi network at a shopping mall, a comparison that carries at least some

facial appeal. A person can choose not to log on to the mall's Wi-Fi network and will still be able to shop, make phone calls, or otherwise remain available to be contacted while in the mall. There is no requirement that a person connect to the shopping mall's network in order to participate in what the mall has to offer.

However, the comparison is not entirely apt. The use of the internet at Moravian (and, I suspect, at most, if not all, post-secondary institutions) is not just a luxury for the students. Access to the internet is a mandatory part of the academic curriculum.[13] A student cannot complete the curriculum and earn a degree without using the internet. Thus, at Moravian at least, being able to connect to the internet is not truly optional as it is at shopping malls or at one's local coffee shop. Thus, the Superior Court's comparison to networks provided at shopping malls ultimately fails to offer a satisfactory rationale for rejecting the presence of an expectation of privacy here.

The Superior Court also discerned a resemblance or similarity between Moravian's Wi-Fi network and security cameras. I do not. In their ability to collect data, security cameras typically are limited to the visual range of the lens. An exterior security camera cannot locate a person inside of the building or in a particular room of that building. An expansive Wi-Fi network can. Moravian has over 1,300 access points on campus that can collect data and locate a person fairly accurately anywhere on campus. Such expansive coverage even can reveal the location of a person inside of a dorm room. Perhaps most importantly, security cameras cannot identify a person by name, whereas the records created by accessing the Wi-Fi network can. Due to the robust reach and capacity of such a network, it is not comparable to the much more limited powers of a security camera.

---

13 *Id*.

I also am unpersuaded by the primary basis upon which the lower courts attempted to distinguish cellular towers from the Wi-Fi network at issue here: to wit, Moravian's Wi-Fi network has a geographical reach smaller than that of cellular towers. That the Wi-Fi network extends only to the outer rim of Moravian's campus is of no moment. For purposes of an expectation of privacy analysis, the Wi-Fi network at issue here functionally operates the same as the cellular towers in *Carpenter*. It is smaller only in scale. For constitutional purposes, the two are one and the same. When a user connects to one of Moravian's 1,300 access points, a record is created, just as a record is created when a cell phone connects to a tower. Such records are "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216. Once compiled, those Wi-Fi records can be used to establish both where a person was on campus and when that person was there. As in *Carpenter*, these records create a "detailed and comprehensive record of the person's movements," *id.* at 2217, and an "exhaustive chronicle of location information." *Id.* at 2219.

Not all connections to Wi-Fi networks are the same, and not all such networks will create an expectation of privacy in one who connects to that network. But, here, the combination of: (1) the expansiveness of the network on Moravian's campus, and (2) the fact that the student must connect to, and use, the internet to successfully complete the academic curriculum is in some ways analytically akin to the cellular towers at issue in *Carpenter*. Hence, it is enticing to jump to the same conclusion that the Supreme Court reached in *Carpenter*, and to hold that Dunkins had a reasonable expectation of privacy in the records created by connecting to the Wi-Fi access points. But there is one key difference between the cases that precludes that leap. In *Carpenter*, the Supreme Court's ruling was driven by the fact that a powered-on cell phone is a part of life, one that simply cannot reasonably just be turned off. A cell phone user cannot prevent or avoid the

creation of the tower records that track his or her every movement. But a Moravian student can.

There is no dispute that, as our comparisons above suggest, Moravian's Wi-Fi network, when accessed and used to its fullest extent, can provide the same detailed, comprehensive location records as cellular towers. In that capacity, the network undoubtedly *could* give rise to a reasonable expectation of privacy, and, going forward, post-secondary schools must proceed with caution if they elect to compel a waiver of rights but not provide students with the ability to control how and when they connect to the network and create historical records of such use. However, notwithstanding the prevalence of the internet in our society, and notwithstanding the fact that Moravian students are bound to use the internet to complete the academic curriculum, students are not required to use Moravian's network to its fullest extent. Students have the ability to limit their use of the network, and thereby to control the records that are created documenting their location at any given time. Automatic connection to Moravian's network, at all times and in any location on campus, is an elective option. Dunkins, or any other student, can forego the automatic connection feature, and can instead choose to log on, and then log off, manually. Doing so, students can control, and, thus, limit, the data generated pertaining to their movements and locations. Unlike the cell phone user, who the *Carpenter* Court determined had no power to control creation of the records, Moravian students have that option.

By opting not to automatically connect to the network at all times, a Moravian student could avoid the generation of records that can provide law enforcement authorities with a "detailed and comprehensive record of the person's movements," *id.* at 2217, and could prevent the "exhaustive chronicle of location information." *Id.* at 2219. Dunkins, who was made aware of, and assented to, the potentiality that data could be

provided to the police, chose nonetheless to automatically connect, a non-mandatory feature on Moravian's campus. In this regard, Moravian's Wi-Fi network differs substantially and materially from the circumstances that undergirded the Supreme Court's decision in *Carpenter*. Accordingly, finding *Carpenter* to be distinguishable, I would hold that Dunkins did not have an expectation of privacy in the records generated by his voluntary use of Moravian's Wi-Fi network.[14]

III.

The Majority assumes, for argument's sake, that Dunkins had an expectation of privacy, and proceeds directly to the question of whether Dunkins waived any expectation that he may have had. Relying upon nothing more than the fact that Dunkins signed the waiver form, the Majority concludes that, by affixing his signature to the page, Dunkins "specifically agreed" to forfeit any expectation of privacy in the data created and collected through his use of the Wi-Fi network. Maj. Op. at 20. By that purported consent, Dunkins "provide[d] clear intent to relinquish his expectation of privacy" in the records and "further acquiesced to the consequences" of that decision. *Id.* Thus, the Majority has "little

[14] The Superior Court also determined that *Carpenter* did not apply because law enforcement used a different data collection technique than did the police in *Carpenter*. There, police sought all records from any tower generated by Carpenter's particular cell phone number. Here, the Superior Court observed, police requested a "tower dump," which is a request for all data created at a particular location, whether a cellular tower or Wi-Fi access point. Because the *Carpenter* Court declined to address the constitutional implications of a "tower dump," the Superior Court inferred that the difference in collection technique had constitutional significance, and thus rendered the cases distinguishable from one another. Dunkins only minimally addresses the distinction, and makes no substantive argument pertaining to the constitutionality of "tower dumps." *See* Brief for Dunkins at 49. However, because I would find that *Carpenter* does not apply, I will not address whether the collection technique used here was a "tower dump," or whether "tower dumps" are constitutional, because Dunkins had no expectation of privacy in those records, however they were collected.

difficulty" concluding that Dunkins abandoned whatever privacy rights he had in the Wi-Fi records. *Id.* In my view, examination of the validity of the waiver requires more than merely locating a signature in the handbook.

In addition to assuming the existence of an expectation of privacy, the Majority assumes another thing: the enforceability of the compulsory waiver in the Computing Resources Policy. In its brief waiver analysis, the Majority neither identifies nor analyzes any applicable case law, from this Court or from any other court, that would support its assumption that the compulsory waiver was legally binding, particularly when the result of that waiver results in evidence to be used in a criminal case. The Majority merely highlights Dunkins' assent to the specific language in the policy, and proceeds to conclude that he voluntarily gave up his rights. I would not assume that the compulsory waiver was legally valid before so readily concluding that Dunkins voluntarily waived his rights.

I have found no cases from this Court that specifically address the validity of the type of compulsory waiver policy used by Moravian in its Computing Resources Policy. However, there are two federal cases that are facially relevant to this case: *Medlock* and *Adkinson*. Although not binding on this Court,[15] they nonetheless are worthy of discussion.

In *Medlock*, Zachary Medlock, a sophomore at Indiana University, agreed, as a condition of living by choice in a university dormitory, to allow graduate-student inspectors to perform health and safety inspections of his dorm room. *Medlock*, 738 F.3d at 869. Inspectors searched Medlock's room and found a tube containing marijuana sitting on Medlock's desk. The inspectors reported the discovery to the campus police. Police officers reported to the dorm room and conducted a more thorough inspection, which

---

[15] *See Commonwealth v. Laird*, 726 A.2d 346, 359 n.12 (Pa. 1999).

revealed several other violations of the student code of conduct, including the presence of a six-foot tall marijuana plant in Medlock's closet. The officers then obtained a search warrant and found additional drug paraphernalia. *Id.* at 869-70.

Medlock was arrested and charged with drug offenses, which later were withdrawn for unknown reasons. However, the university suspended Medlock for one year. After the suspension and his reinstatement as a student, Medlock filed a civil rights action under 42 U.S.C. § 1983, arguing, among other things, that the search of his dormitory room was unconstitutional.

The United States Court of Appeals for the Seventh Circuit rejected the argument. First, the court noted that, because the criminal charges were withdrawn, the only proceedings at issue were disciplinary hearings, at which the Fourth Amendment's exclusionary rule has no applicability. *Medlock*, 738 F.3d at 871 (citations omitted). Second, the court held that, even if the Fourth Amendment applied, there was no violation because Medlock had consented in advance to the search of his room. The court explained that Medlock "could have lived off campus and thus have avoided being governed by the code. He chose to trade some privacy for a dorm room. His expulsion amounted to holding him to his contract." *Id.* at 872.

In *Adkinson*, Adkinson and three confederates robbed a T-Mobile store in Indiana and then a Verizon store in Kentucky. *Adkinson*, 916 F.3d at 608. The crew proceeded to rob nine more stores, including three more T-Mobile stores. *Id.*

T-Mobile investigated the robberies by performing "tower dumps," in an effort to identify the perpetrators. *Id.* The information obtained from the dumps informed T-Mobile that only one T-Mobile user was near the robberies at the relevant time. Adkinson was an authorized user on that account. T-Mobile, reviewing the time-stamped cell tower records, determined that Adkinson traveled from Chicago to the Indiana-Kentucky border,

approached the Verizon store the day it was robbed, and then returned to Chicago. T-Mobile turned this information over to the FBI.

T-Mobile's user agreement contains a provision that allows T-Mobile to disclose information pertaining to its users to "satisfy any applicable . . . legal process or governmental request" or to "protect the rights" or interests of others. The FBI used the information to get an order to access other cell phone records. *Id.* Adkinson was apprehended, charged, and convicted. On appeal to the Seventh Circuit, Adkinson asserted that his cell phone records were unconstitutionally obtained.

In a *per curiam* opinion, the appellate court first held that T-Mobile was not a state actor, meaning that Adkinson had no Fourth Amendment right against T-Mobile. T-Mobile acted in its own interests, and by accepting the information, the Government did not ratify T-Mobile's actions or otherwise convert them into state action. Second, the court held that, even if T-Mobile was a state actor, there still was no Fourth Amendment violation, because Adkinson consented to the tower dump and to the subsequent disclosure of the dumped records to the Government when he agreed to the conditions of the user agreement. *Id.* at 610-11.

Medlock, which was premised upon a waiver in a student handbook, and *Adkinson*, which involved a dump of cellular phone records, bear at least facial relevance to this case. These cases appear to support the contention that a third-party constitutionally can demand a waiver of privacy rights as a condition to the receipt of contracted services. However, there is reason to hesitate in applying these authorities here. For one thing, this pair of federal cases, one of which is a *per curiam* decision, do not bind this Court. Moreover, in *Medlock*, the seized incriminating evidence was admitted solely at an administrative disciplinary proceeding, not at a criminal trial. For that reason alone, at least one other court has distinguished *Medlock*. *See State v. Rodriguez*, 521 S.W.3d 1,

17 (Tex. Crim. App. 2017). Finally, in neither *Medlock* nor *Adkinson* did the Seventh Circuit contemplate the validity of the purported waivers based upon their compulsory nature. The court in both cases assumed without analysis that the waivers were valid and then applied them in the Fourth Amendment context.

As neither *Medlock* nor *Adkinson* are binding or particularly instructive, and with no clear guidance from our own prior decisions, we are left to apply our traditional standards of review for assessing the validity of a waiver of constitutional rights. Typically, we evaluate such a waiver with circumspection:

> While an accused may waive his constitutional right, such a waiver must be the "free and unconstrained choice of its maker", and also must be made knowingly and intelligently. To be a knowing and intelligent waiver[, a] defendant must be aware of both the right and of the risks of forfeiting that right.
>
> Furthermore, the presumption must always be against the waiver of a constitutional right.

Commonwealth v. Monica, 597 A.2d 600, 603 (Pa. 1991) (citations and quotations omitted). In evaluating a waiver of constitutional rights, we must consider the totality of the circumstances. *See Commonwealth v. Scoggins*, 304 A.2d 102, 105 (Pa. 1973) (explaining that "we have always adhered to a totality of the circumstances rule where we consider all factors surrounding the waiver to determine whether it was knowing and intelligent."). In its own summary of the applicable law, the Majority cogently notes that abandonment of constitutional rights is a decision that must be made voluntarily. *See* Maj. Op. at 9-10 (quoting *Commonwealth v. Shoatz*, 366 A.2d 1216, 1220 (Pa. 1976)). To this end, the Majority quotes *Shoatz*, in which this Court specifically explained that "all relevant circumstances existing" at the time of the waiver must be considered to determine whether the person "voluntarily discarded . . . or relinquished" his interest in seized property.

Our precedents, including those relied upon by the Majority, require a contemplation of "all factors surrounding the waiver." *Scoggins*, 304 A.2d at 105. Despite this directive, the Majority contemplates just one fact: Dunkins' signature on the waiver page. The Majority's truncated analysis is akin, in a *Miranda* case, to finding that a confession was valid solely because the defendant signed the *Miranda* form, without any regard for the circumstances and coercive tactics that may have preceded the signature. A signature is but one factor in a totality analysis. It is not the only factor. There is more to consider.

Considering all circumstances in their totality, and, operating first under a presumption against waiver, as we must, the circumstances of this case do not suggest that Dunkins' waiver was knowing, intelligent, or voluntary. The waiver resembles a contract of adhesion more than it resembles a voluntary and intelligent agreement. *See Chepkevich v. Hidden Valley Resort, L.P.,* 2 A.3d 1174, 1190 (Pa. 2010) ("An adhesion contract is a 'standard-form contract prepared by one party, to be signed by the party in a weaker position, usu[ally] a consumer, who adheres to the contract with little choice about the terms.'" (quoting BLACK'S LAW DICTIONARY 342 (8th Ed. 2004)). After years of work building a resume worthy of college acceptance, and after being admitted to the school, a student is provided with a handbook that requires a signature before the student's college career can begin. It is a compulsory agreement. The student, having no ability to negotiate, is in the weakest imaginable position. The student has no choice but to sign the form if he or she wants to be a student at the school.

Under these circumstances, I do not find it as easy as the Majority does to deem waivers such as these to represent a willful and voluntary choice. In actuality, the college effectively strong-arms the students into signing the waiver. Dunkins had no choice but to sign, else he would have been turned away at the campus gate. The facial

involuntariness of these waivers is even more troubling given the fact that it is unlikely that Moravian students fully understand what they are giving up. Students are advised by the waiver form that they are required to forfeit any expectation of privacy in the records and that data may be turned over to the police. It is unlikely, however, that the students understand that the compelled signature would give law enforcement the ability to track their every movement, historically and in near real-time, and to use that information to recreate their travels for purposes of prosecuting them in a criminal trial. More than a rote signature is required to prove that students know what they are forfeiting.

Ultimately, any waiver analysis proves non-dispositive in this particular case, because Dunkins' decision to opt into the automatic connection feature of Moravian's Wi-Fi network precluded him from retaining an expectation of privacy in the records. As such, Dunkins' purported waiver is immaterial. But I cannot agree that Dunkins' signature encompasses the totality of the circumstances. That signature is just one such circumstance, and, standing alone, it does not suffice to overcome the presumption against waiver of constitutional rights. Hence, though I reach the same result as the Majority, I arrive there from a different path.

Justice Donohue joins this concurring and dissenting opinion.