[J-36A-2024, J-36B-2024 and J-36C-2024]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

TODD, C.J., DONOHUE, DOUGHERTY, WECHT, MUNDY, BROBSON, McCAFFERY, JJ.

COMMONWEALTH OF PENNSYLVANIA,	:	No. 98 MAP 2023
	:	
Appellee	:	Appeal from the Order of the
	:	Superior Court at No. 811 MDA
	:	2021 entered on April 28, 2023,
v.	:	Affirming the Judgment of Sentence
	:	of the Northumberland County Court
	:	of Common Pleas, Criminal Division,
JOHN EDWARD KURTZ,	:	at No. CP-49-CR-0000045-2018
	:	entered on March 2, 2021
Appellant	:	
	:	ARGUED: May 14, 2024
COMMONWEALTH OF PENNSYLVANIA,	:	No. 99 MAP 2023
	:	
Appellee	:	Appeal from the Order of the
	:	Superior Court at No. 421 MDA
	:	2023 entered on April 28, 2023,
v.	:	Affirming the Judgment of Sentence
	:	of the Northumberland County Court
	:	of Common Pleas, Criminal Division,
JOHN EDWARD KURTZ,	:	at No. CP-49-CR-0001236-2018
	:	entered on March 2, 2021
Appellant	:	
	:	ARGUED: May 14, 2024
COMMONWEALTH OF PENNSYLVANIA,	:	No. 100 MAP 2023
	:	
Appellee	:	Appeal from the Order of the
	:	Superior Court at No. 429 MDA
	:	2023 entered on April 28, 2023,
v.	:	Affirming the Judgment of Sentence
	:	of the Northumberland County Court
	:	of Common Pleas, Criminal Division,
JOHN EDWARD KURTZ,	:	at No. CP-49-CR-0001479-2018
	:	entered on March 2, 2021
Appellant	:	
	:	ARGUED: May 14, 2024

OPINION ANNOUNCING THE JUDGMENT OF THE COURT

JUSTICE WECHT **DECIDED: December 16, 2025**

In recent decades, "the internet has developed . . . from a useful, but not essential, tool into an integral and indispensable aspect"[1] of American life. Among the internet's many functions, perhaps the most useful or familiar is the ability to gain immediate answers to the myriad questions that arise in our daily lives. When we need information—whether it is the mileage between our home and our travel destination, the hour that a business closes, or the treatment for a self-diagnosed medical condition—we "Google" it.[2] So when John Kurtz wanted to know the home address for K.M.—a woman that he later kidnapped and raped—he did just that. He "Googled" it. In a subsequent investigation into Kurtz' crimes, the Pennsylvania State Police ("PSP") obtained a search warrant for a substantial quantity of Google's records and thoroughly examined them. The records revealed Kurtz' Google search for K.M.'s address.

Kurtz argues that the PSP failed to establish probable cause individualized to him, as is constitutionally required to support issuance of a search warrant. Before a person can challenge the validity of a search warrant, he or she first must demonstrate an expectation of privacy in the area searched. In this case, we must decide whether a

---

[1] *Commonwealth v. Dunkins*, 263 A.3d 247, 258 (Pa. 2021) (Wecht, J., concurring and dissenting).

[2] To "Google" something is "to use the Google search engine to obtain information about (someone or something) on the World Wide Web." *Google*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/google (last visited Jan. 13, 2025). There are, of course, other search engines, such as Yahoo!, Bing, and Duck, Duck, Go, just as there are facial tissues other than "Kleenex," bandages other than "Band-Aid," and cola beverages other than "Coke." For the reasons discussed below, our analysis here is limited to general, unprotected internet searches, *i.e.*, open the search engine, type words into the search bar, and tap the "Enter" key. Our discussion does not extend to searches in which users take additional steps to protect their privacy. The constitutional implications of a user's attempts to conduct more secure searches are not before the Court today.

person who conducts general, unprotected internet searches has an expectation of privacy in the records generated by those searches.[3] We conclude that the average search engine user—including Kurtz—does not. Accordingly, we do not reach Kurtz' probable cause challenge, and we affirm the judgment below.

On July 19, 2016, K.M. went to bed after her husband departed to work his midnight shift as a correctional officer. K.M. had been sleeping for some time when she was awakened by her barking dogs. K.M. arose from bed, and, as she walked through the house, a man jumped out of an empty bedroom. He bound her hands with zip ties, gagged her, and blindfolded her. He dragged her out of the house and put her in his vehicle. He drove her to a nearby camper, where he raped her vaginally and anally. He then released her in a cornfield and fled.

K.M. walked to a nearby residence, and police were called. PSP troopers responded and took K.M. to a local hospital. There, medical personnel retrieved sperm from K.M.'s body. DNA testing did not yield a match with any known person.

Without a DNA match, and given K.M.'s inability to identify her assailant, the PSP's investigation into the identity of the perpetrator was at risk of reaching a dead-end. PSP investigators decided to look in one last place: the internet. Investigators had no evidence that the perpetrator used a computer or Google's internet search engine to assist him in committing his crimes, but they believed that he had researched K.M.'s name or address beforehand. This belief arose from several factors. First, K.M.'s home was remote, and could not be seen by those passing by on the road, which suggested that the assault was not random. Second, the circumstances suggested that the perpetrator was familiar with K.M. and the layout of her residence. Investigators thought that the perpetrator might have orchestrated the crime "possibly after seeing her in the

---

[3] *See Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

community."[4] Third, investigators believed that, "because many sexual offenders are predominantly fantasy driven, there was a basis to conclude that K.M.'s assailant may have been stalking her over a period of time."[5] Fourth, investigators surmised that, because K.M. was attacked while her husband was at work, the assailant may have researched her personal life and schedule.

Relying upon these deductions, PSP investigators applied for, and obtained, a "reverse keyword search warrant" for the records that Google generated during the week prior to the assault. The warrant was not directed at a specific person's activity, but instead targeted all searches performed on Google's search engine for K.M.'s name or address. Over one year later, Google informed the PSP that it had reviewed its records and had found that someone had conducted two searches for K.M.'s address a few hours before the attack. PSP investigators then were able to determine that the same IP address was used for both searches, and that the IP address was associated with Kurtz' residence.

PSP investigators now had reason to suspect that Kurtz was the perpetrator. Investigators tracked Kurtz around the clock, and soon found a connection between him and K.M: Kurtz was a correctional officer at the same facility where K.M.'s husband worked. Shortly thereafter, PSP investigators observed Kurtz toss a cigarette butt onto the pavement in the parking lot of a store. Investigators retrieved the butt, obtained a viable DNA sample from it, and then compared that sample to the one taken from K.M.'s body. The samples matched. PSP troopers arrested and interrogated Kurtz, who not only confessed to K.M.'s rape and abduction, but also admitted to assaulting four other victims. He then showed troopers where three of those victims lived. Kurtz was charged

---

4 *Commonwealth v. Kurtz*, 294 A.3d 509, 523 (Pa. Super. 2023).

5 *Id.* at 523-24 (citing Aff. of Probable Cause, 9/14/2016; R.R. at 173a).

in separate cases with offenses related to each of the five victims. All of the cases were consolidated for trial.

Kurtz filed a motion to suppress the evidence derived from the search of Google's records. The trial court denied the motion, and the case proceeded to a jury trial. The jury found Kurtz guilty on all counts. The trial court subsequently sentenced Kurtz to fifty-nine to two hundred and eighty years in prison. Kurtz appealed.

The Superior Court affirmed.[6] The panel held that Kurtz could not demonstrate an expectation of privacy in the records of his internet searches.[7] The court explained that such demonstration requires an actual subjective expectation of privacy that society is prepared to recognize as reasonable.[8] The court noted that, under the third-party doctrine, a person can forfeit a legitimate expectation of privacy in "property that is voluntarily provided to others as he has taken the risk that that information would be conveyed by the third party to the government."[9] The panel observed that the third-party doctrine has been applied to computer files, digital records, emails, and chat room messages.[10]

The panel concluded that Kurtz could not establish an expectation of privacy in either the records of his Google searches of K.M.'s home address or his IP address. The court explained that, "[b]y typing in his search query and pressing enter, [Kurtz] affirmatively turned over the contents of his search to Google, a third party, and voluntarily

---

6 *Id.* at 516, 536.

7 *Id.* at 522.

8 *Id.* at 520 (citing *Commonwealth v. Kane*, 210 A.3d 324, 330 (Pa. Super. 2019)).

9 *Id.* (citing *Commonwealth v. Pacheco*, 263 A.3d 626, 636, 636 n.10 (Pa. 2021)).

10 *Id.* at 521 (collecting cases). The Superior Court panel emphasized that federal courts have uniformly held that people lack an expectation of privacy in their IP addresses. *Id.*

relinquished his privacy interest in the search."[11] The panel opined that its ruling was buttressed by Google's Privacy Policy, "which specifically allowed for the company to turn over search results when requested by law enforcement and which he assented to by using the company's search service."[12]

Kurtz filed a petition for allowance of appeal. We granted review in order to determine "whether the Superior Court erred in concluding that an individual does not have a reasonable expectation of privacy in his or her electronic content, particularly in his or her private internet search queries and IP address?"[13]

The Fourth Amendment to the United States Constitution provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[14]

---

[11] *Id.* at 522.

[12] *Id.* (footnote omitted). In the alternative, the panel held, even if Kurtz could demonstrate an expectation of privacy in the records of his searches, the warrant was supported by constitutionally adequate probable cause. *Id.* at 523-24.

[13] *Commonwealth v. Kurtz*, 306 A.3d 1287 (Pa. 2023) (*per curiam*). We also granted *allocatur* on the issue of whether "probable cause may be established to support a search warrant to Google, Inc. requesting the content of an individual's private internet search queries where the suspect is unknown and no evidence is presented establishing that Google, Inc. was used in the planning or commission of the crime." *Id.* Because we find that Kurtz lacks an expectation of privacy in the records, we do not reach the probable cause question. *See Commonwealth v. Enimpah*, 106 A.3d 695, 702 (Pa. 2014) ("[I]f the evidence shows there was no privacy interest, the Commonwealth need prove no more[.]").

[14] U.S. CONST. amend. IV. We begin with a discussion of federal constitutional law because, if an expectation of privacy exists under that rubric, the Supremacy Clause would divest us of any need to address the issue as a matter of state constitutional law. Moreover, in his analysis under Article I, Section 8 of the Pennsylvania Constitution, Kurtz argues, in part, that, because the Supreme Court of the United States recognized an expectation of privacy in digital data in *Carpenter v. United States*, 585 U.S. 296 (2018), this Court should do the same.

The Fourth Amendment is not implicated in every governmental action that yields evidence or information that will be used in a criminal trial. Nor does it give every person impacted by that action the right to seek a remedy. The Amendment's protections are triggered only when a "search" (or "seizure") occurs, which, in constitutional parlance, refers to any state action that intrudes upon a "constitutionally protected reasonable expectation of privacy."[15] If the person challenging the use of the evidence does not have a reasonable expectation of privacy in the place where the evidence was found, then there was no "search" under the Fourth Amendment, which, in turn, means that the contested governmental action has no constitutional significance. This is because the Fourth Amendment "protects people, not places,"[16] and "reflects the recognition of the Framers that certain enclaves should be free from arbitrary government interference."[17] Courts do not categorize Fourth Amendment places according to their physical characteristics, but instead must determine whether a person has a legitimate expectation of privacy in the particular "enclave" involved.

In his famous concurrence in *Katz v. United States*, Justice Harlan explained that, for a person to demonstrate an expectation of privacy, "there is a twofold requirement."[18] First, that person must "have exhibited an actual (subjective) expectation of privacy and, second, . . . the expectation [must] be one that society is prepared to recognize as

---

15 *Katz*, 389 U.S. at 360 (Harlan, J., concurring); *see also New York v. Class*, 475 U.S. 106, 112 (1986) (explaining that a "State's intrusion into a particular area, whether in an automobile or elsewhere, cannot result in a Fourth Amendment violation unless the area is one in which there is a constitutionally protected reasonable expectation of privacy") (internal quotation marks omitted)).

16 *Katz*, 389 U.S. at 351.

17 *Oliver v. United States*, 466 U.S. 170, 178 (1984).

18 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

reasonable."[19] Not all expectations of privacy implicate the Fourth Amendment in the same way. The Supreme Court of the United States has stressed "the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the republic."[20] The home stands as "the most essential bastion of privacy recognized by the law,"[21] and warrants the Fourth Amendment's most rigorous protections.[22] "[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[23] On the other end of the privacy spectrum, items left in plain view do not implicate the Fourth Amendment at all.[24] The same is true for items found by police when searching "open fields" that surround a

---

19 *Id.* Justice Harlan's articulation of the expectation of privacy test endures to this day, and it is the one that we use to evaluate search and seizure claims under the Pennsylvania Constitution as well. *See Commonwealth v. Alexander*, 243 A.3d 177, 192 (Pa. 2020).

20 *Oliver*, 466 U.S. at 178 (quoting *Payton v. New York*, 445 U.S. 573, 601 (1980)).

21 *Minnesota v. Carter*, 525 U.S. 83, 106 (1998) (Ginsburg, J., dissenting); *see also Griffin v. Wisconsin*, 483 U.S. 868, 883 (1987) (Blackmun, J., dissenting) ("The search in this case was conducted in petitioner's home, the place that traditionally has been regarded as the center of a person's private life, the bastion in which one has a legitimate expectation of privacy protected by the Fourth Amendment.").

22 *See Payton*, 445 U.S. at 586 (recognizing that, as "a basic principle of Fourth Amendment law[,] searches and seizures inside a home without a warrant are presumptively unreasonable" (internal quotation marks and footnote omitted)); *Coolidge v. New Hampshire*, 403 U.S. 443, 474-75 (1971) (explaining that, under the Fourth Amendment, "a search or seizure carried out on a suspect's premises without a warrant is *per se* unreasonable, unless the police can show . . . the presence of exigent circumstances") (internal quotation marks and footnote omitted); *see also Commonwealth v. Romero*, 183 A.3d 364, 397 (Pa. 2018) (OAJC).

23 *United States v. Karo*, 468 U.S. 705, 714 (1984).

24 *Horton v. California*, 496 U.S. 128, 133-34 (1990).

person's home.[25] A middle ground may be found in the automobile, which, at least under federal law, falls between a house and items left exposed to the public eye.[26] Under the Fourth Amendment, a person has a reduced expectation of privacy in an automobile and, thus, police officers may search a vehicle based upon nothing more than the ability to articulate probable cause.[27] Unlike a house, no warrant is required before a vehicle can be searched, but, unlike the plain view doctrine or the open fields doctrine, there must at least be a demonstration of probable cause before an automobile search can proceed.

In this case, PSP investigators obtained a search warrant for records pertaining to internet searches. The advent and proliferation of the internet has brought about new and complicated challenges for courts and law enforcement agencies alike:

> 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

---

[25] *Oliver*, 466 U.S. at 177; *Hester v. United States*, 265 U.S. 57, 59 (1924) (holding that the "special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects' is not extended to the open fields").

[26] *See Carroll v. United States*, 267 U.S. 132, 149 (1925); *United States v. Ross*, 456 U.S. 798, 809 (1982). *But see Alexander*, 243 A.3d at 150 (holding that Article I, Section 8 of the Pennsylvania Constitution requires both probable cause and exigent circumstances before a vehicle can be searched by police without a valid search warrant).

[27] *See California v. Carney*, 471 U.S. 386, 392 (1985).

> appointments, to conducting academic research, to operating every aspect of a business.[28]

However, that the internet is now commingled with most, if not all, of our personal and professional activities does not mean that a person automatically has a constitutionally reasonable expectation of privacy in its general usage. This holds true even when the internet usage occurs within a person's home, a place that, as noted above, typically is associated with the Fourth Amendment's most stringent protections.

At the heart of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[29] In his renowned dissent in *Olmstead v. United States*, Justice Louis Brandeis put it this way:

> The makers of our Constitution . . . conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect[] that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[30]

But, the pedestal upon which the Fourth Amendment places the home crumbles when "a person knowingly exposes [private material] to the public."[31] While "a man's home is, for most purposes, a place where he expects privacy," that privacy does not extend to those "objects, activities, or statements that he exposes to the plain view of outsiders."[32] Such shared materials are "not protected because [that person has

---

28 *Dunkins*, 263 A.3d at 268 (Wecht, J., concurring and dissenting).

29 *Silverman v. United States*, 365 U.S. 505, 511 (1961) (citation omitted); *accord Gooding v. United States*, 416 U.S. 430, 462 (1974) (Marshall, J., dissenting) ("[T]here is no expectation of privacy more reasonable and more demanding of constitutional protection than our right to expect that we will be let alone in the privacy of our homes during the night.").

30 *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

31 *Katz*, 389 U.S. at 351.

32 *Id.* at 361 (Harlan, J., concurring) (internal quotation marks omitted).

exhibited] no intention to keep them to himself."[33] This principle—known in the law as the "third-party doctrine"—holds that, generally, a person lacks an expectation of privacy in information or materials when that person exposes them to a third party. This doctrine proceeded on a steady course in federal search and seizure jurisprudence for decades until recent years, when it has by necessity undergone significant adaptation in light of advanced developments in modern digital technologies.

The third-party doctrine emerged prominently in the mid-to-late 1970s in two United States Supreme Court decisions: *United States v. Miller*[34] and *Smith v. Maryland*.[35] In *Miller*, the Court held that a suspect under investigation for tax-related crimes lacked an expectation of privacy in his bank records because a person can "assert neither ownership nor possession" of such documents.[36] The records that typically are deposited with banks include checks, *i.e.*, negotiable instruments that are disseminated in commerce, and, thus, exposed to, the public, and account statements that contained information that was "exposed to [bank] employees in the ordinary course of business."[37] Because such documents voluntarily were placed in the hands of a third party, the Court held, a person has no expectation of privacy in them. A consumer availing himself of the bank's services necessarily had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government."[38]

---

33 Id.

34 425 U.S. 435 (1976).

35 442 U.S. 735 (1979).

36 *Miller*, 425 U.S. at 440.

37 *Id.* at 442.

38 *Id.* at 443.

The Court returned to the third-party doctrine three years later in *Smith.* There, government officials—without a warrant—used a pen register[39] to record all of the numbers that were dialed on a landline telephone located inside a robbery suspect's home.[40] The petitioner challenged the use of the pen register on Fourth Amendment grounds. The Court held that the government's use of the device was not a "search" for Fourth Amendment purposes, as the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial."[41] The Court noted that, typically, telephone users know that they must convey numbers to the phone company, which, in turn, uses those phone numbers for "a variety of legitimate business purposes."[42] Thus, "[a]lthough subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[43] To the extent that the petitioner did, in fact, believe he had an expectation of privacy in those numbers, the Court explained, that expectation was not one that society would deem reasonable: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[44]

The third-party doctrine plodded along steadily until the progression of modern technology forced the Court to begin to examine third-party interactions in a different light.

---

39 "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 161 n.1 (1977).

40 *Smith*, 442 U.S. at 737.

41 *Id.* at 742.

42 *Id.* at 743.

43 *Id.*

44 *Id.* at 743-44.

First came *United States v. Jones*, in which the Court, relying upon trespass principles, held that attaching a GPS device to a vehicle and using satellite technology to track the operator's movements in that vehicle constituted a "search" under the Fourth Amendment.[45] Justice Sotomayor joined the Court's opinion, but authored a concurring opinion that planted the seeds for what the third-party doctrine has since become. Justice Sotomayor expressed concern that, in light of technology's increasing role in contemporary society, the doctrine may have outlived its usefulness. She believed that it had become "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[46] Justice Sotomayor perceived the third-party doctrine as "ill suited" to the "digital age" because most, if not all, people now "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[47] "People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[48] Justice Sotomayor's concerns notwithstanding, the *Jones* Court as a whole did not re-examine the viability of the third-party doctrine. But then came *Carpenter*.

In 2011, police officers arrested four men who perpetrated a string of robberies at various electronics stores across Michigan and Ohio.[49] While confessing to these offenses, one of the arrested men provided to the FBI names and cellular telephone

---

45 565 U.S. 400, 404 (2012).

46 *Id.* at 417 (Sotomayor, J., concurring).

47 *Id.*

48 Id.

49 *Carpenter*, 585 U.S. at 301.

numbers of fifteen other participants in what was revealed to be a larger criminal organization. One of those additional suspects was Timothy Carpenter. In an effort to collect CSLI[50] records related to Carpenter's cellular device over a four-month period during which the robberies occurred, prosecutors secured two court orders under the Stored Communications Act. In order to obtain such records under that statute, a prosecutor must present "specific and articulable facts showing that there are reasonable grounds to believe" that the records were "relevant and material to an ongoing criminal investigation."[51] FBI agents executed the two court orders and obtained CSLI records connected to the suspects' cell phones covering a period of approximately one-hundred and thirty days. From that data, prosecutors and law enforcement agents examined almost 13,000 geographical points—over one hundred points per day—that enabled them to determine Carpenter's location and reconstruct his movements during that time.[52]

After being arrested and charged, Carpenter sought to suppress the CSLI records. Carpenter asserted that collection of the CSLI records constituted a "search" under the Fourth Amendment that could be executed only upon a showing of probable cause, not upon the lesser "reasonable grounds" standard required by the Stored Communications Act. The District Court denied his motion. At trial, the prosecutor used the CSLI records

---

50 CSLI is an acronym for "cell-site location information." The *Carpenter* 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 300-01.

51 18 U.S.C. § 2703(d).

52 *Carpenter*, 585 U.S. at 302.

in order to establish that Carpenter was located near the scenes of the robberies at the time they occurred. He was convicted of a litany of crimes and sentenced to over one hundred years in prison.[53]

The Supreme Court of the United States granted *certiorari* to decide "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."[54] As noted above, in order to constitute a "search" for constitutional purposes, the challenged intrusion must enter into an area within which a person has a reasonable expectation of privacy. Accordingly, in order to answer the question presented, the Court first had to ascertain whether a person has a reasonable expectation of privacy in CSLI records that track a person's public movements.[55] If so, the use of the lesser "reasonable grounds" standard would be unconstitutional, as it would fall below the requirements of the Fourth Amendment.

The Court observed that the collection of CSLI records is a novel law enforcement function that does not necessarily fit neatly within the Court's existing precedents. Rather, "requests for cell-site records lie at the intersection of two lines of cases."[56] In the first of these cases, the Court historically has held that, in general, a person does not have a reasonable expectation of privacy in his or her physical location or movements while in public.[57] By moving openly about in public, the Court explained, a person voluntarily

---

53 *Id.* at 302-03.

54 *Id.* at 300.

55 *Id.* at 304.

56 *Id.* at 306.

57 *Id.* (citing *United States v. Knotts*, 460 U.S. 276, 281 (1983)).

exposes his movements to others.[58] However, this rule is not absolute. Indeed, the rule does not apply when law enforcement officers go beyond naked-eye observations of what a person exposes to the public and, instead, engage is more extensive or intrusive surveillance. For instance, the Court noted, *Jones* held that a warrant was required when evidence was obtained by installing a GPS device surreptitiously on a vehicle. Such surveillance enables law enforcement officers to track a person's every movement over a period of time.[59]

The second line of decisions arose in the Court's third-party doctrine cases, *Miller* and *Smith*. As discussed above, these cases stand generally for the proposition that a person has no reasonable expectation of privacy in information that he or she voluntarily discloses to another person. The theory is that, once a person conveys information to someone else, that person "assume[s] the risk" that the information later will be turned over to law enforcement officers.[60]

The *Carpenter* Court considered whether, and, if so, how, these two lines of cases applied to this "new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."[61] The Court discerned some similarities between the collection of CSLI data and the data produced by the GPS device in *Jones*. This suggested to the Court that *Jones* had at least facial applicability, as both types of data are "detailed, encyclopedic, and effortlessly compiled."[62] On the other hand, the Court explained, the third-party doctrine seemed to have little, if any, relevance in regard

---

58 *Id.*

59 *Id.* at 307 (discussing *Jones*).

60 *Smith*, 442 U.S. at 745.

61 *Carpenter*, 585 U.S. at 309.

62 *Id.*

to the collection of CSLI data. Although the doctrine applies logically to bank records and telephone numbers, "it is not clear whether its logic extends to the qualitatively different category of cell-site records."[63] "After all," the Court continued, "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."[64]

The Court rejected the view—proffered by the Government and endorsed by Justice Kennedy in dissent—that CSLI data were business records and that, as such, they fell comfortably within the confines of the third-party doctrine. This argument failed "to contend with the seismic shifts in digital technology" that now allow for an all-encompassing compilation of a person's public movements "for years and years."[65] "There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[66] Applying the third-party doctrine to CSLI data would not be a "straightforward application" of the doctrine, but instead would be a "significant extension of it to a distinct category of information."[67]

Critically, the Court explained, the third-party doctrine does not negate entirely any expectation of privacy that a person has in information that he or she knowingly shares with another. Such a person retains an expectation of privacy, but it is a reduced expectation. The Court stressed that a diminished privacy interest is not the equivalent

---

63 *Id.*

64 *Id.*

65 *Id.* at 313.

66 *Id.* at 314.

67 *Id.*

of no privacy interest at all. The Fourth Amendment does not "[fall] out of the picture entirely."[68] The *Carpenter* Court discerned "no comparable limitations on the revealing nature of CSLI," and, thus, rejected a mechanical application of the third-party doctrine.[69] 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*."[70]

The Court stressed that the third-party doctrine does not reflexively apply merely because a cell phone user voluntarily has allowed the data to be created. "Cell phone location information is not truly 'shared' as one normally understands the term."[71] The Court explained:

> 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.[72]

Thus, the Court concluded, the third-party doctrine did not preclude an expectation of privacy in CSLI records. "Given the unique nature of cell phone location records," regardless of "[w]hether the government employs its own surveillance technology as in

---

68 *Id.* (quoting *Riley v. California*, 573 U.S. 373, 392 (2014)).

69 Id.

70 *Id.* at 315.

71 *Id.*

72 Id.

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."[73] Consequently, obtaining CSLI data from a wireless carrier is a "search" for purposes of the Fourth Amendment, and a valid search warrant is a necessary prerequisite to that "search."[74]

The decision was "a narrow one," the Court explained, limited to the type of data collected (and to the method of collecting such data) in that case.[75] The Court cautioned that the decision should not be read to disturb the ordinary application of the third-party doctrine as outlined in *Smith* and *Miller*.[76]

Resolution of the central question in this case—whether a person has an expectation of privacy in his or her unprotected internet searches—rests upon whether such actions are governed by *Carpenter*'s "narrow" rejection of the third-party doctrine, or fall instead under the traditional third-party doctrine. The Court's deviation from the traditional doctrine in *Carpenter* in large part was predicated upon the inextricable relationship between the contemporary person and his or her device. Because the Court considered mobile devices to be "indispensable to participation in modern society,"[77] the *Carpenter* Court held that their use in public is an unavoidable part of modern life. As such, the Court held, a person does not make a voluntary choice to place CSLI generated by cell phone use into the hands of third parties. Rather, such transmission happens automatically.

---

73 *Id.* at 309-10.

74 *Id.* at 316.

75 Id.

76 *Id.*

77 *Id.* at 315 (citing *Riley*, 573 U.S. at 385).

A reasonable comparison can be made between the prevalence of the internet in modern society and the prevalence of cell phone usage. Such similarity, however, does not mean that they are one and the same for purposes of the third-party doctrine. Rather:

> *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.[78]

It is beyond cavil that the internet is extensively intertwined with nearly every aspect of contemporary life. We use it to schedule appointments, to communicate with friends and former schoolmates, to play games, to hold meetings, and to conduct research on any number of topics. The list goes on and on. However, unlike smart phones, the internet is not a "feature of human anatomy."[79] The use of the internet is not involuntary, as cell phones have become. To the contrary, every time a person logs on to the internet, that person makes a choice. She chooses to input data into a network owned and operated by an internet service provider. While users (reasonably) may believe that their searches are private, they nonetheless willingly transmit data to a third party whenever they type terms into a search engine and hit the "Enter" key. Unlike the

---

78 *Dunkins*, 263 A.3d at 269 (Wecht, J., concurring and dissenting).

79 *Riley*, 573 U.S. at 385.

cell phone user who cannot avoid creation of a data trail, the internet user can avoid or minimize the creation of such records by using other methods of research. A person seeking a restaurant reservation can telephone or visit the establishment rather than using the internet to book it. Someone hoping to learn more about dinosaurs or galaxies can conduct research in print materials at the library.[80] Persons seeking privacy can

---

[80] The Dissent dismisses these illustrative examples as "fantasy," largely because printed phone books and encyclopedias are no longer as prevalent as they once were. Diss. Op. at 14. A misconception that pervades the Dissent's analysis is its conflation of convenience and necessity. The two are distinct. That it might be faster or more convenient to use Google to find show times at a movie theater does not mean that a Google search is the only way to find that information. When a person seeks information or assistance, that person makes a choice. No one forces a person to select Google. When that person clicks on Google, there is a consequence: a loss of privacy. The fact that taking the time to shield one's browsing history, use a VPN, or resort to telephone or print resources might be incrementally less convenient does not change that consequence.

The Dissent misconstrues the larger point, as well as the breadth of this Court's ruling in *DeJohn*. The Dissent asserts that we are creating a new privacy rubric, one in which privacy rights depend upon the unavailability of more convenient options. *See* Diss. Op. at 15. That is incorrect. Google tells the user that it is collecting and sharing data. Nearly every website or cellular phone application informs the user that it will collect data using "Cookies," and invariably requires the user to agree to that collection before proceeding. The average internet user receives unambiguous, unavoidable, explicit notice that his or her internet data is not private. While the Dissent insists against all the evidence that there still exists a privacy right in that information, it is plain and obvious that there is not. The situation might be different if the user was forced into using Google, or if Google was the only option available. But neither is the case. We are not required to ignore the fact that users are told that they have no privacy in their internet usage, and that they press on anyway.

To state this obvious conclusion is not to attempt an implicit and silent overruling of *DeJohn*. Nothing we say here has any impact on that case. Under Pennsylvania's Constitution, a person still has an expectation of privacy in his or her bank records. The expectation of privacy analysis is not a one-size-fits-all approach. Each circumstance requires consideration of the unique factors attending that circumstance. Bank records and pen registers are not the same as internet usage data, public movements, cell phone usage information, conversations in phone booths, etc. We address only the situation before us.

(continued…)

shield their browsing history.[81] The point is that the data trail created by using the internet is not involuntary in the same way that the trail created by carrying a cell phone is.[82]

That one should not expect absolute privacy in the routine use of the internet should not come as a surprise. It is common knowledge that websites, internet-based applications, and internet service providers collect, and then sell, user data. Nearly every time a person opens an internet-based application for the first time on a smart phone or home computer, he or she is notified of such expansive data collection and is given the option to opt out of it. It is not at all infrequent that a person searches online for a product today, only to receive electronic advertisements for that same product tomorrow. The

---

The Dissent's criticism flows from its misreading of *DeJohn*. The Dissent points to no place in *DeJohn* or *Melilli* where this Court rejected the third-party doctrine *in toto*. That this Court declined to apply that doctrine to the unique circumstances of those cases does not mean that the Court "specifically rejected" its existence as a whole. *Id.* That one commentator appears to share the Dissent's view, *see id.* at 13 n.11, does not alter the fact that this Court has never once said, in *DeJohn*, *Melilli*, or any other case, that we reject the third-party doctrine entirely as a matter of Pennsylvania law.

[81] There are a number of ways in which a user can hide or protect their browsing history. For instance, most modern internet browsers offer an "incognito" or "private browsing" mode. *See How To Hide Browsing History—Complete Guide*, TRIPWIRE https://www.tripwire.com/state-of-security/hide-browsing-history-complete-guide (last visited July 14, 2025). A person also can use a private VPN, regularly delete his or her browsing history, opt out of data-collection efforts by websites or applications, and limit or manage the "Cookies" stored by websites. *Id.*

[82] The Dissent professes avoidance of the central question in this case under federal law. *See* Diss. Op. at 8 n.8 ("I do not address the Majority's conclusion . . . under the Fourth Amendment . . . ."). Nonetheless, the Dissent asserts that, like the cellular devices in *Carpenter*, the use of Google is "equally 'a pervasive and insistent part of daily life' such that using Google 'is indispensable to participation in modern society.'" *Id.* (quoting *Carpenter*, 573 U.S. at 385). The Dissent confuses Google for the internet. As we noted above, *supra* at 1, the internet is indeed an essential tool in modern society. Google is just one of the many services that make navigating the internet quicker and easier. Google is not the internet itself. The Dissent's approach is akin to treating a Ford vehicle as the American roadway because Ford (hypothetically) is the most popular automaker in the nation. Google is one of many internet applications that a person voluntarily chooses to use, and it is one that specifically informs each user that it collects and shares the user's data.

point is that, even the ordinary, everyday use of the internet provides strong indicators that there is no privacy in the terms or information that the user voluntarily enters into a search engine.

In the case before us, Google went beyond subtle indicators. Google expressly informed its users that one should not expect any privacy when using its services. Under the "Privacy" tab situated on the bottom right-hand corner of Google's home page, at the time of the searches at issue in the case *sub judice*, Google informed its users of the following:

> We collect information about the services that you use and how you use them. . . .
>
> We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). . . .
>
> When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes . . details of how you use our service, such as your search queries[,] . . . [and IP] address. . . .
>
> We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to . . . meet any applicable law, regulation, legal process or enforceable request.[83]

Thus, when a person performs a Google search, he or she is aware (at least constructively) that Google collects a significant amount of data and will provide that data to law enforcement personnel in response to an enforceable search warrant.[84] For

---

83 *See* Commonwealth's Exhibits 4 and 5.

84 The Dissent characterizes Google's Privacy Policy as an agreement between the user and Google that limits Google's use of the records of the user's search. Diss. Op. at 27. Because Google agrees to disclose the collected material only when "reasonably necessary" to meet any "enforceable governmental request," the Dissent insists that the (continued…)

present purposes, what Google does with that information, including the standards it imposes upon itself before providing that information to investigators, is irrelevant.[85] For Fourth Amendment purposes, what matters is that the user is informed that Google—a third party—will collect and store that information. When the user proceeds to conduct

---

user can claim an expectation of privacy in whatever material Google compiles. The Dissent misses the point. The point is not that Google has agreed to turn that data over to a third party only in certain circumstances. The point is that Google itself is the third-party. Once a user agrees voluntarily to Google's collection of the information, there no longer is a reasonable expectation of privacy in that information. What Google agrees to do with that information is irrelevant. By that juncture, the user already has exposed that information to a third-party: Google. That banks, cell phone companies, cable companies, etc., also collect and store data, *see id.*, does not mean that everyone who uses those services can claim an expectation of privacy in those records. As *Carpenter* and *DeJohn* make clear, it is the voluntariness of the exposure of materials to those third-parties that controls the inquiry.

[85] The Dissent misunderstands, and then serially misapprehends, our use of the term "irrelevant" here. The Dissent reads this sentence as a sweeping assertion that we believe Google's Privacy Policy is irrelevant entirely to the constitutional expectation of privacy analysis. Diss. Op. at 2 n.1, 26-27. To the contrary. Like the Dissent, we find the Policy highly relevant. We do "take[] it into account in determining whether a user has a reasonable expectation of privacy in the searches on the engine." Diss. Op. at 2. The Policy expressly informs its users: (a) that it collects information about the Google services that the user accesses and about how the user utilizes those services; (b) that it collects data about the hardware or device through which the user accesses Google's services; and (c) that it automatically collects and stores information related to the specific search terms employed by the user as well as that user's IP address. Google does not hide the ball about what comes next. The Policy specifically instructs its users that it will take that vast, and at times personal, body of data, and share it with additional third parties, including law enforcement under certain circumstances. Thus, in no uncertain terms, every person that logs on to Google knows that Google will collect personal information about that user and then share that information with third parties. One hardly can maintain that, under these circumstances, he or she reasonably expects privacy in that information.

What is "irrelevant" here is not what Google expressly tells its users, but what Google ultimately does with that information. By that point, with knowledge and permission, the user already has exposed the information to a third party: Google. Where Google then proceeds to send that information is irrelevant. Any privacy interests were breached the moment a user knowingly and voluntarily allowed Google to collect the data. As we note throughout this opinion, a user who wants to keep such material private has options. That user does not have to click on Google.

searches with that knowledge, he or she voluntarily provides information to a third party. This express warning, in tandem with the more indirect indicators noted above, necessarily precludes a person from claiming an expectation of privacy in his or her voluntary internet use. Any such claim is not one that society would find objectively reasonable.[86]

That a person accesses the internet from inside his or her home is of no moment. In *Smith*, the United States Supreme Court rejected this very proposition with regard to in-home phone calls:

> [T]he site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.[87]

The same must be said when a person accesses the internet from inside the privacy of his or her home, as opposed to, say, a public library: it "make[s] no conceivable difference."[88] Like the telephone user in *Smith*, the internet user voluntarily must "convey" information to his internet service provider.

For these reasons, Kurtz's contention that, pursuant to *Carpenter*, he has a cognizable expectation of privacy under the Fourth Amendment, is erroneous. To the contrary, for purposes of federal law, the traditional third-party doctrine applies, and, thus,

---

86 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

87 *Smith*, 442 U.S. at 743.

88 Id.

Kurtz lacked an expectation of privacy in the material he voluntarily shared while using the internet.

Kurtz also claims an expectation of privacy under the Pennsylvania Constitution.[89] The argument fares no better.[90] Although Kurtz presents a full *Edmunds*[91] analysis, his

---

[89] Article I, Section 8 of our Commonwealth's charter states that the "people shall be secure in their persons, houses, papers and possessions from unreasonable searches and seizures, and no warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause . . . ." PA. CONST. art. 1, § 8.

[90] In Pennsylvania, a person charged with a possessory offense has "automatic standing" to challenge a search or seizure because "the charge itself alleges an interest sufficient to support a [] claim [under Article I, Section 8 of the Pennsylvania Constitution.]" *Commonwealth v. Sell*, 470 A.2d 457, 468 (Pa. 1983) (citation and internal quotation marks omitted). However, standing only "entitles a defendant to a review of the merits of his suppression motion without a preliminary showing of ownership or possession in the premises or items seized." *Enimpah*, 106 A.3d at 698. It does not relieve the challenger of the obligation to demonstrate a societally recognized expectation of privacy. Stated otherwise, "while a defendant's standing dictates when a claim under Article I, [Section] 8 may be brought, his privacy interest controls whether the claim will succeed." *Id.* at 699.

[91] *See Commonwealth v. Edmunds*, 586 A.2d 887 (Pa. 1991). In *Edmunds*, this Court created a four-part rubric to assist in evaluating claims that Pennsylvania's Constitution affords greater protections than its federal counterpart. An *Edmunds* analysis requires courts to examine: (1) the text of the provision in our Constitution; (2) the history of the provision, including cases from Pennsylvania courts interpreting that provision; (3) relevant cases from other jurisdictions; and (4) relevant policy considerations. *Id.* at 895. An *Edmunds* analysis is unnecessary when no "departure" claim is presented. *See Commonwealth v. Bishop*, 217 A.3d 833, 840 (Pa. 2019). Where, as here, the argument is a straightforward state constitutional claim, one that is consistent with, not departing from, federal law, no such analysis is necessary. Because Kurtz maintains that he has an expectation of privacy in his Google searches under both our Constitution and under the Fourth Amendment pursuant to *Carpenter*, there was no need for him to structure his argument under the *Edmunds* rubric. For that reason, we focus upon the crux of his argument instead of formally proceeding through the four *Edmunds* factors.

argument under Article I, Section 8 rests primarily upon this Court's decisions in *Commonwealth v. DeJohn*[92] and *Commonwealth v. Melilli*.[93]

In *DeJohn*, this Court declined to follow the United States Supreme Court's "dangerous precedent"[94] in *Miller*, and held instead that, as a matter of state constitutional law, a person in Pennsylvania enjoys an expectation of privacy in his or her bank records.[95] This was, in part, because a person's use of the banking system (at least in the 1970s) was "not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[96] Thus, much like the United States Supreme Court did in *Carpenter*, this Court held that, in a "realistic approach to modern economic realities,"[97] providing information to banks was an involuntary and unavoidable aspect of life, and thus outside the reach of the third-party doctrine.

At issue in *DeJohn* were bank records that police obtained through two subpoenas *duces tecum*.[98] The Commonwealth did not defend the legality of the subpoenas. The Commonwealth argued instead that DeJohn lacked standing to challenge the subpoenas. To this end, the Commonwealth "urge[d] this Court to *apply* the *Miller* holding."[99] This Court passed on that invitation. Indeed, this Court "decline[d] to follow [*Miller*] when

---

92 403 A.2d 1283 (Pa. 1979).

93 555 A.2d 1254 (Pa. 1989).

94 *DeJohn*, 403 A.2d at 1289.

95 *Id.* at 1291.

96 *Id.* at 1289 (quoting *Burrows v. Super. Ct. of San Bernardino Cnty.*, 529 P.2d 590, 596 (Cal. 1974)).

97 *Id.* at 1291.

98 *Id.* at 1287.

99 *Id.* (emphasis added).

construing the state constitutional protection against unreasonable searches and seizures."[100] We instead found the California Supreme Court's decision in *Burrows* to be "more persuasive than . . . *Miller*."[101] The *Burrows* Court held that a person has an expectation of privacy in his or her bank records, because a person's use of a bank in modern society is involuntary.[102] The *Burrows* Court did not refuse to adopt the third-party doctrine. That Court held only that banking fell outside the parameters of the third-party doctrine. The *DeJohn* Court held precisely the same thing.

This Court similarly declined to apply the third-party doctrine in *Melilli*, a case involving law enforcement use of pen registers. We explained that Pennsylvania's "long history of affording special protection to the privacy interest inherent in a telephone call"[103] produced a "marked trend of our state law to bring intrusions into telephone communications within the confines of an expectation of privacy under the State Constitution and thereby be subject to the requirements demonstrating probable cause."[104] However, the expectation of privacy that this Court recognized in *Melilli* was

---

100 *Id.* at 1289. The Dissent interprets this line from *DeJohn* differently. In the Dissent's view, when this Court "decline[d] to follow [Miller]," *id.*, we actually refused to "adopt" the third-party doctrine entirely as a matter of state constitutional law. Diss. Op. at 12. Conspicuously absent from the Dissent's novel characterization of *DeJohn* is any reference to any point in the *DeJohn* opinion where this Court actually said that. To the contrary, the Dissent's support for its broad, textually unsupportable view of that case is the same quote upon which we rely: this Court's decision to "decline to follow" *Miller*. That we chose not to follow the United States Supreme Court's ruling in one circumstance—bank records—does not mean that we simultaneously and *sub silentio* eschewed the third-party doctrine in every conceivable circumstance.

101 *Id.* at 1290.

102 *Burrows*, 529 P.2d at 596.

103 *Melilli*, 555 A.2d at 1258 (quoting *Commonwealth v. Beauford*, 475 A.2d 783, 790 (Pa. Super. 1984)).

104 *Id.*

limited to "telephone communications," which, as a matter of state constitutional law, "are regarded as private."[105]

DeJohn and *Melilli* are distinguishable from the instant case. As we explained above, the use of the internet is not an inextricable and involuntary aspect of our daily life in the same way that mobile phones have become or, as the *DeJohn* Court held, the banking system was. That the internet is helpful, readily available, and convenient does not render its use involuntary in such a way that a person today has no choice but to rely upon it and, derivatively, has no choice but to share information with third parties.

The *Melilli* Court recognized that telephone calls warrant strenuous privacy protections, in large part because of their intimate and confidential nature. Telephone calls involve two parties and often concern personal topics. The same cannot be said about general internet use. The average user logs on and transmits data about countless topics to internet service providers. Surfing the web to access news or to make purchases

---

[105] *Id.* at 1259. The Dissent contends that *Melilli*, like *DeJohn*, demonstrates an outright and all-encompassing refusal to adopt the third-party doctrine. As in its discussion of *DeJohn*, the Dissent does not point to any portion of this Court's *Melilli* decision that says that. That this Court declined to apply the doctrine to a person's phone calls does not mean that this Court rejected the doctrine in its entirely and in perpetuity. At best, *DeJohn* and *Melilli* hold that the third-party doctrine does not apply to bank records and telephone calls. This hardly suggests that the doctrine does not exist in Pennsylvania at all.

There is yet another glaring fallacy in the Dissent's interpretation of these two cases. It is a fallacy with which the Dissent fails to grapple, and for obvious reasons. Had this Court in *DeJohn* "declined to **adopt** [the third-party doctrine] as the framework for the privacy analysis under the state constitution," Diss. Op. at 12-13 (emphasis in original), as the Dissent imagines, resolving *Melilli* would have been perfunctory. This Court would simply have stated that "there is no third-party doctrine in Pennsylvania, as we held in *DeJohn*." Of course, this Court said no such thing, nor could it have done so. Instead, this Court examined whether the third-party doctrine applied to telephone calls. It would be odd indeed for this Court to attempt to ascertain whether a doctrine that does not exist in Pennsylvania applies in Pennsylvania. And that is not what happened. Instead, this Court recognized the existence of the doctrine and declined to apply in that one particular circumstance.

on massive shopping websites while using an unprotected internet browser cannot reasonably be equated to private telephone calls between family members or friends. *Melilli* has no application here.

That two of our precedents reject the application of the third-party doctrine does not mean that a person is guaranteed a broad expectation of privacy in all forms of electronic communication or interaction. To the contrary, a person's actions and effects will be deemed "private, even if they are accessible to . . . others," so long as the person "maintain[s] the privacy . . . in such a fashion that his expectations of freedom from intrusion are recognized as reasonable."[106] A person using a globally-accessible search engine that unambiguously informs its users that it collects and stores data, on an unprotected browser, using access afforded by an internet service provider, has done nothing to "maintain" his or her privacy and has no reasonable "[expectation] of freedom from intrusion."[107]

To be clear, this case is limited to general, unprotected internet use. The result may, in fact, differ if an internet user has taken efforts to secure some degree of privacy. For instance, a user who accesses the internet using a "virtual private network,"[108] who

---

106 *Commonwealth v. White*, 327 A.2d 40, 42-43 (Pa. 1974) (internal quotation marks and citations omitted).

107 *Id.* at 43.

108 A "virtual private network," commonly referred to as a "VPN," is a "digital connection between [a] computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet. This ensures [that the user's] online experiences are private, protected, and more secure." *What is a VPN?*, MICROSOFT, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn (last visited Jan. 29, 2025).

The Dissent deems it "inconceivable" that the government can monitor a person's internet usage, usage that, the Dissent correctly notes, often involves very personal information. Diss. Op. at 21. There are ways to prevent such monitoring. It can be as (continued…)

uses an internet browser that does not collect or share data, or who visits websites that are password-protected, such as those related to one's medical care, might retain a constitutionally recognizable expectation of privacy.[109] That is not what happened in this case. When the average internet user opens an unencrypted internet browser and

---

simple as using a VPN. It can be as simple as accessing the internet through a browser or search engine that does not collect and share private data. Those options are not good enough for the Dissent. In the Dissent's view, because the internet is pervasive in contemporary society, a user should be able to access it at any time, for any purpose, on any browser, without any privacy implications whatsoever. For the Dissent, a user who is told that he should expect no privacy in his searches still may demand a constitutional expectation of privacy in them. To the contrary, when Google expressly informs a person that it will collect and share that person's data, society would not deem reasonable any insistence that the person can claim an expectation of privacy in that data.

[109] The Dissent rejects the manifest reality that there are options available to a person who wishes to protect his privacy and to avoid Google's data collection program. Diss. Op. at 22. For the Dissent, these options are impractical because only "generations reared on internet usage" are capable of navigating the complexities of installing a VPN or typing "Duck, Duck, Go" instead of Google into the search bar. *See id.* at 22 (asserting that the "life vest" of privacy protection options is "being thrown to users of those generations reared on internet usage"). We do not share the Dissent's broad stereotyping of internet users based upon chronological age.

The Dissent's hypothetical scenario also misses the mark. The Dissent asserts that "we would never require a homeowner to purchase a home security system or lock his doors to find that he has a reasonable expectation of privacy in his own home." *Id.* True enough. But the internet user at issue in this case is not the person sitting inside his home with the front door shut. The internet user is more akin to a person sitting on the front porch of that house. The Dissent wants the privacy protections provided by the front door to protect what the person sitting on the front porch exposed to his neighbors. The privacy of the home does not extend that far. It does not protect what the person broadcasts to persons outside the home.

The Dissent contends that this analogy "encapsulates [our] general underestimation of the role that Google plays in society." *Id.* at 25. The Dissent opines without substantiation that there is a "unique sense of security that individuals feel in sharing and searching for information on the machine-based search engine." *Id.* This would be unique indeed. The Dissent forgets that the foundation of every expectation of privacy analysis is the issue of what society would deem reasonable. No reasonable person feels a "sense of security . . . in sharing and searching for information" on a website that specifically informs that very same person that he or she should *not* feel secure in the data created by "sharing and searching for information."

performs a search on a website such as Google, he or she voluntarily enables the creation and collection of data, and, in such circumstances, has no societally recognized expectation of privacy.[110]

For these reasons, Kurtz had no enforceable expectation of privacy in his internet searches. As such, he cannot prevail on a challenge to the validity of the search warrant executed in this case. We affirm.

Justices Dougherty and Brobson join the opinion announcing the judgment of the Court.

Chief Justice Todd files a concurring opinion in which Justices Mundy and McCaffery join.

Justice Mundy files a concurring opinion.

Justice Donohue files a dissenting opinion.

---

[110] At several points, the Dissent appears to respond to an alternative or imaginary version of this Opinion. Hence, notwithstanding that we begin by recognizing at the very outset that "'the internet . . . [is] an integral and indispensable aspect' of American life," *supra* at 1 (quoting *Dunkins*, 263 A.3d at 258 (Wecht, J., concurring and dissenting), the Dissent asserts that we see that tool as "merely convenient but not necessary." Diss. Op. at 2. And although we explicitly discuss Google's privacy policy, *supra* at 26-29 & nn. 85-86, the Dissent claims nonetheless that we deem that policy "irrelevant." Diss. Op. at 2 n.1. The Dissent does not let reality get in its way, proceeding to erect and then knock down additional straw men as it strives to avoid confronting the consequences that attend an internet user's unprotected online search. The Dissent can deride our conclusion as "divorced from reality and blind," *id.* at 2, and as "fantasy," *id.* at 14, but that conclusion arises from a realistic and eyes-open application of our Constitutions to our online lives. The Dissent fulminates over "robust" and "foundational" privacy protections afforded in Pennsylvania, *id.* at 2, and implies that we are here "thoughtlessly relying on [U.S.] Supreme Court precedent . . .," *id.* at 11 n.9, but the fact remains that Pennsylvanians are capable of using platforms other than Google and of utilizing VPNs or other means of protecting their online privacy should they wish to do so.