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

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

DISSENTING OPINION

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

I disagree with the conclusion of the Opinion Announcing the Judgment of the Court ("OAJC") that a person who uses Google's search engine[1] does not have a reasonable expectation of privacy in that activity. The robust privacy protections afforded by the Pennsylvania Constitution demand the opposite conclusion and required law enforcement to obtain a warrant to conduct the search under the circumstances. In reaching its conclusion, the OAJC re-casts our foundational Article I, Section 8 precedent as it pertains to a citizen's protection from government access to information shared with third parties. Under Article I, Section 8, a Google user has a reasonable expectation of privacy in the information shared with Google via internet searches because utilization of the internet search engine to research information is necessary to participate in our technology-driven society and the stored information, in totality, provides a virtual current biography of the user. The OAJC's conclusion that using the search engine is merely convenient but not necessary is both divorced from reality and blind to the societal benefits flowing from ready access to infinite amounts of information available with the technology[2] without fear of undeterred government surveillance.

---

[1] Unlike the OAJC, I limit my analysis to the facts of this case which involves Google searches. Contrary to the OAJC's view that the Google Privacy Policy is irrelevant, in my view, it must be taken into account in determining whether a user has a reasonable expectation of privacy in the searches on the engine. *See* N.T., 5/22/2018 (Commonwealth's Exhibit 4 (Google Privacy Policy (last mod. 6/28/2016) at 4 ("Google Privacy Policy")).

[2] It is fair to debate whether the ability to instantaneously access snippets of information in answer to specific queries is detrimental to acquiring knowledge necessary to fully understand a topic. But the outcome of the debate is purely theoretical. Google and other similarly designed electronic search engines are now ingrained as the global methodology for accessing information. Pragmatically, access to information is beneficial when compared to no alternative.

Because under Article I, Section 8 jurisprudence, the Google user had an expectation of privacy in his searches, I also address the adequacy of the search warrant. Under the facts presented, the affidavit of probable cause fell short of establishing probable cause. Thus, suppression was required as the constitutional remedy for the violation. I would reverse the order of the Superior Court.

I. Background

Google, the leading global search engine, enables internet users to discover information through websites. *See* Amicus Brief for American Civil Liberties Union, ACLU of Pennsylvania, Library Freedom Project, Association of Research Libraries, Freedom to Read Foundation, and Internet Archive ("ACLU's Brief") at 6, 14-15. To retrieve information, users formulate search queries consisting of keywords and enter those queries into the search engine browser. *See* Amicus Brief for Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, and Pennsylvania Association of Criminal Defense Lawyers ("EFF's Brief") at 6. Search engines arrange website content according to algorithms that grade the content on its relevance to the keywords. *Id*. For Google, these algorithms process 99,000 search queries per second and draw from hundreds of billions of websites within Google's virtual collection in order to serve roughly 83% of Americans. *See* ACLU's Brief at 13-15.

Google collects user information irrespective of whether users have signed into their Google accounts. EFF's Brief at 10. When users are signed in, Google stores their search histories and identifying information for eighteen months by default. ACLU's Brief at 17. When users are not signed in to an account, Google retains search histories linked to IP addresses[3] and internet service providers. EFF's Brief at 10. Thus, Google retains

[3] An IP address is shorthand for an "Internet Protocol" address, which is an identifying number assigned to a user by an internet service provider. N.T., 5/22/2018, at 6-7. A user's IP address communicates with websites, such as Google, to facilitate internet (continued…)

a unique and personal "digital trail" for each of its 274.49 million American users. ACLU's Brief at 14, 16. These digital trails capture both the intended and unintended[4] requests for information by Google users. *See* EFF's Brief at 8 (explaining Google's "autocomplete" feature). To avoid leaving a "deeply revealing digital trail," users would have to refrain from internet searches or from using the company's browser entirely. *See* ACLU's Brief at 18.

Reverse search warrants, including "keyword search" warrants,[5] enable police to "identify suspects by demanding that a company comb through its huge repository of data reflecting the public's interactions with its services." *Id*. at 2-3. Unlike traditional search warrants that target specific individuals or accounts, reverse keyword search warrants direct independent providers to scan their entire user database for specified search terms within a specified time. *Id*. at 3.

This appeal arises out of the brutal attack and rape of a woman in Northumberland County. We are here because after failing to identify any suspects, the Pennsylvania State Police ("PSP") obtained a keyword search warrant directing Google to produce

---

searches and provides the destination for the return of information from websites to the user. *Id.* at 7-8.

[4] A search can be unintended because modern search engines offer an "autocomplete" feature which predicts search queries based on users' data, such as "geographical location, their past searches, their language," and other trending searches. *See* EFF's Brief at 8. This feature creates personalized suggestions as users type and frequently leads to unintended searches. *Id*. Moreover, as the ACLU points out, even where a user knows the web site she wants to access, "web site addresses—uniform resource locators or URLs—are often too long to memorize[,]" and thus, users invariably turn to Google to make their way to the URL. ACLU's Brief at 14.

[5] The parties' briefs interchangeably use the terms "reverse search," "keyword search," and "reverse keyword search." These terms collectively describe a surveillance technique where law enforcement obtains a warrant directing Google to identify IP addresses associated with specific search terms from designated timeframes based on their search histories.

records identifying which of its 274.49 million users searched the victim's name or home address during the week preceding the attack.[6] Google identified fourteen IP addresses that fit the search terms. By utilizing a directory of IP addresses, the PSP eventually focused the investigation on John Edward Kurtz, who was associated with at least one of the IP addresses, and PSP brought charges against him for this attack and other attacks that were identified in the course of further investigation. Kurtz moved to suppress the evidence obtained through the search warrant, which the trial court denied, finding that Kurtz did not have an expectation of privacy in the content of his Google searches or his IP address. Trial Court Opinion, 5/17/2021, at 4. The case proceeded to trial.

---

[6] The affiant, Trooper Joel Follmer, identified the "premises and/or person to be searched" as "Google Inc: Support/Legal Investigations: 1600 Amphitheartre [sic] Parkway, Mountain View California, who transparently conducts business in Northumberland County, Pa[.]" Application for Search Warrant at 1. For the "items to be searched for and seized" the affiant referred to Attachment A:

"Attachment A"

1. Google Historical Records related to Google Search Queries and Google Image Search Queries of the searched key phrase and/or image of "[Victim's first and last name]" between dates of July 13, 2016 and July 20, 2016.

2. Google Inc.: Support/Legal Investigations for all identifying information associated with any and all identities or IP addresses associated with the Google Search Queries for the key phrase and/or image of "[Victim's first and last name]".

3. Google Historical Records related to Google Search Queries and Google Maps Search Queries of the searched key phrase and/or address of "70 Schreck Rd. Milton, PA" between July 13, 2016 and July 20, 2016

4. Google Inc.: Support/Legal Investigations for all identifying information associated with any and all identities or IP addresses associated with the Google Search Queries for the key phrase and/or address "70 Schreck Rd. Milton, PA"

* The information requested in this Attachment should be provided either on 8.5x11-inch paper printouts or, where maintained in electronic form, via e-mail, to: [The affiant].

Application for Search Warrant, Attachment A.

On October 14, 2020, a jury found Kurtz guilty of, inter alia, rape, kidnapping, attempted rape, and attempted kidnapping, involving several victims, and he was sentenced to 59 to 280 years of imprisonment. *Id*. On appeal, the Superior Court affirmed Kurtz's judgment of sentence and rejected his arguments that the trial court erred in denying suppression. The Superior Court found that Kurtz lacked a reasonable expectation of privacy in his internet searches and his IP address and, in the alternative, that there was adequate probable cause to justify the warrant. *Commonwealth v. Kurtz*, 294 A.3d 509, 522-24 (Pa. Super. 2023).

Kurtz subsequently filed a petition for allowance of appeal and this Court granted appeal of two issues, namely:

> 1. In an issue of first impression, 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?
>
> 2. In an issue of first impression, whether the Superior Court erred in finding that 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?

Commonwealth v. Kurtz, 306 A.3d 1287 (Pa. 2023) (per curiam).

II. Expectation of Privacy

This Court granted allowance of appeal to determine whether an individual has a reasonable expectation of privacy in his internet search queries and IP address so as to require law enforcement to obtain a warrant. A defendant has two ways to prove that a

search implicates the constitutional warrant requirement.[7] Historically, courts utilized a property-based assessment considering principles of common-law trespass to determine whether a search had occurred. *United States v. Jones*, 565 U.S. 400, 405, 411 n.8 (2012) (providing that the federal constitution protects against trespassory searches of the items enumerated therein (persons, houses, papers and effects)). Kurtz does not assert that this is a search based on a property-based interest in his Google search queries. Instead, he is focused on a test developed in the 1960s in *Katz v. United States*, 389 U.S. 347 (1967). The *Katz* Court addressed circumstances where law enforcement used a special listening device to overhear an individual's conversation in a phone booth, circumstances which did not lend themselves to a property-based assessment. Therefore, the *Katz* Court applied a new inquiry to determine whether a search implicates the constitutional warrant requirement. Justice Harlan articulated the emergent rule: "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id*. at 381 (Harlan, J., concurring). The expectation of privacy test requires "a balancing of the societal interests involved." *Commonwealth v. Peterson*, 636 A.2d 615, 619 (Pa. 1993) (internal citations omitted).

Once a defendant raises a suppression motion premised on a violation of the Fourth Amendment or Article I, Section 8, the Commonwealth bears the burden of proving that the search or seizure was constitutional. *Commonwealth v. Enimpah*, 106 A.3d 695

[7] Notably, "searches and seizures conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well delineated exceptions." *Minnesota v. Dickerson*, 508 U.S. 366, 372 (1993). The Commonwealth here obtained a warrant and did not raise any exceptions to the warrant requirement. Instead, it asserted that Kurtz lacks a reasonable expectation of privacy in his search information. Thus, it succeeds in proving the constitutionality of the search only if it demonstrates that Kurtz lacks a reasonable expectation of privacy or that the warrant was constitutionally sound.

(Pa. 2014) (affirming the grant of suppression because the Commonwealth refused to present evidence at the suppression hearing claiming that its obligation was not triggered until the defendant met his "threshold" burden of proving that he had an expectation of privacy). In addressing suppression motions, courts first consider whether a warrant was constitutionally required by addressing whether there was a search within the meaning of the Fourth Amendment or Article, I, Section 8. *Commonwealth v. Rekasie*, 778 A.2d 624, 628 (Pa. 2001) (stating that before addressing probable cause, "we must initially determine whether Rekasie held a reasonable expectation of privacy"). If there is no expectation of privacy, then the Constitutional protections against unreasonable searches are not implicated.

Kurtz claims that both the Fourth Amendment to the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution protect his privacy from government intrusion in his Google searches. Significantly, and as I later discuss, this Court departed from the federal constitutional approach to searches for information in the possession of third parties, deciding instead that Article I, Section 8 provides greater protection than the Fourth Amendment. Having rejected the federal constitutional approach decades ago, Fourth Amendment jurisprudence is of little relevance to our inquiry.[8] Thus, I look to our

[8] Thus, I do not address the OAJC's conclusion that under the Fourth Amendment a Google user would have no expectation of privacy in information the user shares with Google. However, I am not convinced that this conclusion is correct given the High Court's decision in *Carpenter*, where it declined to extend the third-party doctrine to the collection of cell-site location data from an individual's cell phone company based, in part, on its determination that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter v. United States*, 585 U.S. 296, 315 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). The OAJC and I agree that the internet is an indispensable tool in modern society. OAJC at 2. Without access, the internet is useless. Google is the dominant search engine in the United States, accounting for 85%-90% of the search engine market share at various points in the last year. *Search Engine Market Share United States of America October 2024 – October 2025*, STATCOUNTER https://gs.statcounter.com/search-engine-market-share/all/united-states-of-
(continued…)

Charter to determine whether Kurtz had a reasonable expectation of privacy in his internet search queries.

The protections in the Pennsylvania Constitution now embodied in Article I, Section 8, were established fifteen years prior to the promulgation of the Fourth Amendment. *Commonwealth v. Edmunds*, 586 A.2d 887, 896 (Pa. 1991). Indeed, the federal Bill of Rights borrowed heavily from our state Declarations of Rights. *Id*. The Declaration of Rights in the Pennsylvania Constitution was part of the Commonwealth's original Constitution and has appeared in every iteration since. *Id*. As first adopted, the text of Article I, Section 8 protected the people's "right to hold themselves, their houses, papers and possessions free from search and seizure[.]" *Id*. at 896 (citing PA. CONST., cl. 10 (1776)). The modern version was adopted in 1790, and "has remained untouched for two hundred years, with the exception of the words 'subscribed by the affiant,' which were added by the Constitutional Convention of 1873." *Id*. at 897 (internal citation omitted). The original purpose of Article I, Section 8 was to abolish "general warrants" used to conduct "sweeping searches of residences and businesses, based upon generalized suspicions." *Id*. Though there was a time when interpretation of the Fourth Amendment and Article I, Section 8 ran parallel, this ended by 1973, when Pennsylvania case law "began to reflect a clear divergence from federal precedent." *Id*. In diverging from Fourth Amendment jurisprudence to find stronger protections under Article I, Section 8, this Court issued various decisions emphasizing that Article I, Section 8 "is meant to embody a

---

america#:~:text=Table_content:%20header:%20%7C%20Search%20Engines%20%7C%20Percentage,Yahoo!%20%7C%20Percentage%20Market%20Share:%203.2%25%20%7C (last visited Nov. 24, 2025). Given its overwhelming dominance, Google is equally "a pervasive and insistent part of daily life" such that using Google "is indispensable to participation in modern society." *See Carpenter*, 585 U.S. at 315. The contrary perspective of the OAJC is untethered to the realities of everyday life in households throughout this Commonwealth.

strong notion of privacy, carefully safeguarded in this Commonwealth for the past two centuries." *Id.* at 898.

Relevant to the issue before us, in *Commonwealth v. DeJohn*, 403 A.2d 1283 (Pa. 1979), this Court had the first opportunity to consider whether the federal third-party doctrine applied to Article I, Section 8. The federal third-party doctrine provides generally that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to [g]overnment authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 442-43 (1976) (internal citations omitted). In *Miller*, the United States Supreme Court ruled that an individual did not have an expectation of privacy in bank records because checks, financial statements and deposit slips "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id*. Analysis under the third-party doctrine turns, in large part, on whether an individual "voluntarily conveyed" information to a third-party. In *Smith v. Maryland,* 442 U.S. 735 (1979), the High Court found no expectation of privacy in the numbers that an individual dialed on his phone because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information[,]" and thus, "assumed the risk that the company would reveal to police the numbers he dialed." *Id*. at 744-45. More recently, in *Carpenter*, again focusing on the voluntariness of the conveyance of information, the Court determined that cell phone location information is not voluntarily exposed by a cell phone user because, inter alia, cell phones create these records by means of their operation, "without any affirmative act on the part of the user beyond

powering up" and "there is no way to avoid leaving behind" the digital trail. *Carpenter*, 585 U.S. at 315-16.[9]

Returning to *DeJohn*, which was decided in the wake of *Miller*'s treatment of bank records and the articulation of the third-party doctrine, this Court addressed subpoenas issued to Mellon Bank for "copies of all information pertaining to accounts, or application for account, made by" the DeJohns, and "all original records pertaining to personal cash reserve account application, and original new account card" for the DeJohns. *DeJohn*, 403 A.2d at 1287. This Court concluded that *Miller*—which held that a depositor lacks an expectation of privacy and therefore may not challenge the seizure of her bank records—was "dangerous precedent" and declined to follow it. *Id*. at 1289.

The *DeJohn* Court rejected the premise that engaging in banking activities was voluntary, instead requiring an examination of the activity in the context of its place in the

---

[9] For completeness, it is relevant to note that the foundation of Fourth Amendment third-party doctrine has been called into question. *See, e.g.*, *Carpenter*, 585 U.S. at 342-43 (Thomas, J., dissenting, joined by Alito, J.) (advocating for dissolution of the *Katz* framework). The voluntariness standard itself has been called into question, *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring) (arguing to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"), and redefined, *Carpenter*, 585 U.S. at 315 (suggesting new threshold question for voluntariness, i.e., whether the activity is "indispensable to participation in modern society").

While pertinent, this Court has warned against defining our citizens' rights using federal benchmarks in *Pap's A.M. v. City of Erie*, 812 A.2d 591 (Pa. 2002). We cautioned "[a]s a matter of policy, Pennsylvania citizens should not have the contours of their fundamental rights under our charter rendered uncertain, unknowable, or changeable, while the U.S. Supreme Court struggles to articulate a standard to govern a similar federal question." *Id*. at 611. That states should scrupulously avoid unnecessarily and thoughtlessly relying on Supreme Court precedent when addressing privacy rights of their citizens is a lesson that should have been learned from exclusively relying on federal privacy rights in the area of reproductive autonomy. *Roe v. Wade*, 410 U.S. 113 (1973), overruled by *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022). Our Charter's robust protection of privacy rights deserves continuous application and development.

realities of modern society. The *DeJohn* majority highlighted that the California Supreme Court departed from the *Miller* analysis in *Burrows v. Superior Court of San Bernadino County*, 529 P.2d 590 (Ca. 1974). *Id*. at 1289-90. The Court quoted the *Burrows* Court's observation that engaging in banking is not entirely volitional because it is essentially a requirement of modern society. We also agreed with the *Burrows* Court's commentary that the "totality of bank records provides a virtual current biography," and to give access to this information to law enforcement "opens the door to a vast and unlimited range of very real abuses of police power." *Id*. (citing *Burrows*, 529 P.2d at 596). We emphasized that "judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new [electronic] devices." *Id*. (citing *Burrows*, 529 P.2d at 596). We also highlighted that under *Miller*'s logic, nothing would stop law enforcement from obtaining this information in the complete absence of criminal suspicions. *Id*. We deemed *Burrows* "more persuasive than the simplistic proprietary analysis" of *Miller*. *Id*.

DeJohn teaches that notwithstanding a third-party's access to information, an individual's privacy interest extends to those areas of societal activities that are not entirely volitional because of the mandates of participating in modern society and where the collection of those records, in totality, "provides a virtual current biography." *Id*. at 1289-90 (quoting *Burrows*, 529 P.2d at 595). *DeJohn* rejected the unexamined "voluntariness" standard of *Miller,* the first of the duo of United States Supreme Court cases establishing the third-party doctrine, by holding that bank records were protected by Article I, Section 8 notwithstanding third-party access. The *DeJohn* Court was not concerned with whether there were alternatives to banks and bank accounts to participate in commerce. It was not a question of whether an individual had a choice to use banks instead of cash or money orders to conduct business. The *DeJohn* Court took a realistic

approach to determining whether the activity was an embedded function in modern society. If so, the participation and resultant transfer of information was "not entirely volitional." *Id*. at 1289.

Contrary to the OAJC's rendition of this Court's holding, the *DeJohn* Court did not merely decline to apply the acontextual third-party exception to the warrant requirement; it declined to **adopt** it as the framework for the privacy analysis under the state constitution. *Compare* OAJC at 27-28 (stating that *DeJohn* held that banking fell outside the parameters of the third-party doctrine) *with DeJohn*, 403 A.2d at 1289 ("As we believe that *Miller* establishes a dangerous precedent, with great potential for abuse, we decline to follow that case when construing the state constitutional protection against unreasonable searches and seizures."). The OAJC's view that *DeJohn* only rejected an application of the third-party doctrine and not the doctrine itself, OAJC at 27-28, is baseless.[10] *Miller* set the parameters for what has come to be known as the third-party doctrine based on the unexamined notion of the voluntariness of sharing information with a third party. Rejecting the analysis of *Miller*, this Court established its own analytical framework to address whether citizens of this Commonwealth retain a reasonable expectation of privacy in their records when they are held by a third-party. This Court outright rejected "the simplistic proprietary **analysis**, supposedly rejected in *Katz* …, used

[10] Consistent with my view, and contrary to the position taken by the OAJC, Professor Stephen E. Henderson categorizes Pennsylvania as one of eleven states that reject the federal third-party doctrine. He lists it alongside California, whose *Burrows* opinion was the basis for *DeJohn*. Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 (2006).

by the court in *Miller*" because it found the *Burrows* analysis "in recognizing modern electronic realities … more persuasive." *DeJohn*, 403 A.2d at 1290 (emphasis added).[11]

The OAJC's examination of the expectation of privacy in Google search inquiries purportedly under our Constitution is antithetical to *DeJohn*'s admonition to take into account modern electronic realities when determining whether participation in the activity results in the loss of the expectation of privacy. First, the OAJC's basic premise that Pennsylvanians can easily resort to print materials in the library and can call to make restaurant reservations rather than using the internet to make bookings[12] is a fantasy. Because of the vast accumulation of information accessible at the fingertips of users, alternative sources of some information have become hard if not impossible to come by. How often do we see physical copies of phone books? Do individual households in Pennsylvania own encyclopedias? Individual households never had access to or the research skills to find and decipher medical journals. The OAJC suggests that Pennsylvanians either forgo research into personal medical questions or find the way to a medical school library research assistant.

But even if every household in Pennsylvania, rich or poor, had unfettered access to every piece of information available through a Google search through alternative means, that would be irrelevant to whether one has an expectation of privacy in the search. Were it adopted, the OAJC's position—that in order to maintain an expectation of privacy in information shared with a third party, the party claiming privacy must

---

[11] *Burrows* predated *Miller* and became the basis for Justice Brennan's dissenting opinion in that case. *Miller*, 425 U.S. at 448-54 (Brennan, J., dissenting) (quoting *Burrows* extensively). Moreover, "it has been the basis upon which other states have rejected the federal [third-party] doctrine." Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third-Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 986 (2007).

[12] OAJC at 21.

demonstrate that the sharing of the information "is the only way" to accomplish the specific task—would implicitly overrule *DeJohn*. *See* OAJC at 21 n.80 ("That it might be faster or more convenient to use Google to find showtimes at a movie theater does not mean that a Google search is the only way to find that information."). Using the OAJC's same logic, a bank account is not the only way to spend, save, or transfer money. Yet the *DeJohn* Court recognized a reasonable expectation of privacy in information shared with a bank based on "a realistic approach to modern economic realities[.]" *DeJohn*, 403 A.2d at 1291. Today, this Court supplants *DeJohn*'s realistic approach to privacy in favor of the rigid and antiquated third-party framework that *DeJohn* specifically rejected. Pursuant to *DeJohn*, it is patently obvious that to function in today's society, the utilization of internet searches is necessary for many daily activities and essential when an individual wants to gain knowledge in new areas. It is beneficial to society when an individual, anywhere, decides to explore new ideas. To suggest that exploring these inquiries on Google means that the government has unfettered access to those thoughts opens the door to vast police abuses that the *DeJohn* Court feared would result from the application of *Miller*.

Not long after *DeJohn*, this Court, in *Commonwealth v. Melilli*, 555 A.2d 1254 (Pa. 1989), addressed the second in the duo of the High Court's third-party doctrine cases, *Smith v. Maryland*, 442 U.S. 735, 749 (1979), where the High Court held that installation of a pen register—a device used to collect a record of telephone numbers dialed by a particular telephone number—was not a Fourth Amendment search because callers voluntarily convey numerical information to the telephone company and expose that information in the ordinary course of business. To understand the *Melilli* Court's rejection of *Smith*, we must start with *Commonwealth v. Beauford*, 475 A.2d 783 (Pa. Super. 1984), where the Superior Court addressed whether a pen register may be installed by law enforcement authorities absent a judicial order based on probable cause. The

intermediate appellate court explained that our constitutional right embodies "a right to privacy older than either the federal or state constitution[,]" "at the foundation of our body politic[,]" that directly comes from the "proud boast of an Englishman that his home was his castle and that as long as he obeyed the law, the King and his army could not enter it against his will." *Beauford*, 475 A.2d at 787 (internal citations omitted). Judge Cirillo, writing for the *Beauford* majority, acknowledged that "we are a long way from castles" given the vast electronic "eyes and ears" the government has at its disposal. *Id*. at 787. "But we still cherish our privacy, and today the constitutional prohibition against unreasonable searches and seizures extends beyond the home to protect the individual against unwarranted government intrusions into any area where the individual may harbor a reasonable expectation of privacy." *Id*.

The Superior Court drew from the "wise counsel" of *DeJohn* in its rejection of the reasoning in *Miller*. *Id*. at 788. The court deemed the practice of installing a pen register an invasion of privacy and rejected the federal standard because it was "convinced that a person picking up a telephone in his home or office fully expects that the number he is about to dial will remain as private as the contents of the communication he is about to have." *Id*. at 789. The court emphasized various criteria: it deemed telephone calls as nearly indispensable tools for business, government, political, social, and personal affairs in modern-day America (a reasoning akin to the nonvolitional nature of the activity); it observed that the vast majority of calls are non-criminal; it highlighted that the Legislature, in enacting anti-wiretap statutes, maintained strict controls over resorts to wiretaps by law enforcement agencies and that the courts followed suit; and it emphasized the legislative

effort "to limit [wiretapping] as much as possible to protect individual rights and give law enforcement the necessary tools[.]"[13] *Beauford*, 475 A.2d at 790.

Five years later, this Court granted review in *Melilli*, 555 A.2d at 1254, to address whether *Beauford* was properly decided and whether there is a good faith exception to the probable cause requirement for pen registers. We answered each question with an eye toward the Pennsylvania Constitution's zealous protection of the right to be left alone. *Id*. The *Melilli* Court observed the "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." *Id*. at 1258. It highlighted that the *Beauford* court "intended to equate telephone numbers with other forms of telephone communication which are regarded as private." *Id*. at 1259. Consistent with that intention, we stated that "[t]elephone activities are largely of one piece, and efforts to create distinctions between numbers and conversational content are constitutionally untenable in our view." *Id*.[14] Having approved of *Beauford*'s

---

[13] The *Beauford* court relied on the Wiretapping and Electronic Surveillance Control Act, 18 Pa.C.S. §§ 5701-5782, highlighting that it "allows wiretapping for police investigative purposes, but only after a strict showing of need by the attorney general or a district attorney before a Superior Court judge." *Beauford*, 475 A.2d at 790 (citing 18 Pa.C.S. §§ 5708-5710).

[14] We are not alone in finding fault in the unexamined notion of voluntariness underlying the rationale of the third-party doctrine cases. *See, e.g.*, *Carpenter*, 585 U.S. at 405 (Gorsuch, J., dissenting) (stating that he does "not agree with the Court's decision today to keep *Smith* and *Miller* on life support"); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (referring to the third-party doctrine as "the [*Lochner v. New York*, 198 U.S. 45 (1905)] of search and seizure law"). Similarly, the Colorado Supreme Court recently held that individuals maintain a reasonable expectation of privacy in their Google search queries. *People v. Seymour*, 536 P.3d 1260, 1272-73 (Colo. 2023). The court relied on Google's use of encrypted databases and stringent measures to prevent unauthorized access; the vast nature of the records revealed by an individual's internet searches; and digital privacy laws evidencing that "society finds an expectation of privacy in digital data to be objectively reasonable[.]" *Id*. at 1270-71 (citing 18 U.S.C. §§ 2701-2703; Colorado Privacy Act, §§ 6-1-1301 to -1313). The court (continued…)

approach, we turned to the Commonwealth's effort to invoke a good faith exception, which we also rejected.

Thus, *Melilli* and *DeJohn* did not merely establish exceptions to the doctrine—they rejected the federal framework. There can be no clearer rejection of the third-party doctrine than the rejection of the analytical framework of the two cases that serve as the foundation for what has come to be known as the third-party doctrine.

Subsequent to *Melilli*, this Court has taken fewer opportunities to independently analyze Pennsylvania Constitutional protections with regard to third-party access, but we have not retreated from our rejection of *Miller* or *Smith*.[15] In *Commonwealth v. Duncan*, 817 A.2d 455 (Pa. 2003), this Court held that a police request for the appellant's name and address from a bank was not a constitutional search. *Duncan*, 817 A.2d at 462-63. We observed that the type of information subject to constitutional protections is the information that reveals the essence of a person's personality, not merely basic identifying information.[16] *Id*. at 458-59. Name and address, the Court explained, are categorically

---

observed that it has long held that the Colorado Constitution "provides greater privacy protections than the Fourth Amendment[,]" and that it had rejected the third-party doctrine. *Id*. "Given the enduring and related privacy concerns presented by a search of an individual's online search history," the court saw "no reason to change course" and determined that Seymour had a reasonable expectation of privacy in the search history linked to his IP address under the Colorado Constitution. *Id*.

[15] In *Commonwealth v. Pacheco*, 263 A.3d 626 (Pa. 2021), for instance, the Court was poised to address such an Article I, Section 8 challenge to cell site location information ("CSLI") sought from a cell phone carrier. The Court ultimately resolved the question of whether an individual has an expectation of privacy in his location and physical movements with the Fourth Amendment, relying principally on the United States Supreme Court determination in *Carpenter* that an individual has a reasonable expectation of privacy in historic CSLI. *Pacheco*, 263 A.3d at 640.

[16] *Duncan* is in tension with our subsequent decisions recognizing the right to informational privacy under Article I, Section 1 of the Pennsylvania Constitution and our decision in *Commonwealth v. Alexander*, 243 A.3d 177 (Pa. 2020). *Duncan* was decided in 2003 and was based on an Article I, Section 8 challenge. In *Pennsylvania State University v. State Employees' Retirement Board*, 935 A.2d 530 (Pa. 2007) (*"Penn State*") (continued…)

different from actual bank records. *Id*. at 462-63. Unlike actual bank records, this information does not reveal a "virtual current biography" of an individual. *Id*. at 463. Notably, the *Duncan* Court made clear that *DeJohn* was not in tension with its conclusion and cited Professor LaFave's commentary that *Miller* was dead wrong. *Id*. at 463 (citing Wayne R. LaFave, *Search and Seizure* (3d ed. 1996), § 2.7(c), at 633). Thus, *Duncan* reaffirmed our rejection of *Miller* and reaffirmed the protection of information that reveals a virtual current biography of a person by revealing her activities.

From *DeJohn*, *Melilli*, and *Duncan* arise clear criteria for addressing whether there is a reasonable expectation of privacy in scenarios where the search warrant is directed to a third-party custodian of information. In Pennsylvania, notwithstanding a third-party's access to information, an individual privacy interest extends to those arenas where an

---

and *Tribune-Review Publishing Co. v. Bodack*, 961 A.2d 110 (Pa. 2008), we held that informational privacy including home addresses was protected by the right to privacy under Article I, Section 1 of our Constitution without any reference to *Duncan*. Later, in deciding that names and home addresses were protected by the Article I, Section 1 right to privacy as implicated by the Right to Know Law, 65 P.S. §§ 67.101-67.3104, we followed *Penn State* and *Bodack*, concluding that *Duncan* and Article I, Section 8 were not relevant to the analysis. *Pa. State Educ. Ass'n v. Commonwealth Dep't of Cmty. & Econ. Dev.*, 148 A.3d 142 (Pa. 2016). Justice Wecht concurred, calling for the Court to take the opportunity to distance itself from *Duncan*. *Id*. at 161 (Wecht, J., concurring) ("In light of the majority's well-reasoned analysis today, it seems quite clear that the above-quoted language from *Duncan* is not faithful to our Constitution and its precedents, at least within the context of Article I, Section 1."). In *Commonwealth v. Alexander*, a search and seizure case, we concluded that the rights recognized in Article I, Section 8 and Article I, Section 1 were intertwined for purposes of the scope of the right to privacy under our constitution. *Alexander*, 243 A.3d at 206-07. Placing Article I, Section 1, and Article I, Section 8 privacy rights into separate silos, as we did in *Penn State*, *Bodack*, and *PSEA* is no longer tenable.

Moreover, contrary to the argument of the Commonwealth, *Duncan* does not extend to the circumstances here to support the proposition that Kurtz did not have an expectation of privacy in his IP address. In *Duncan*, the defendant's name and address were produced as standalone information unconnected to the defendant's bank records. *Duncan*, 817 A.2d at 465. Here, the IP address associated with Kurtz's Google searches was produced as part of his specific Google search history records. *See* Google's Response to Search Warrant, 11/29/2017, at 2-3.

individual's engagement is not entirely volitional because of the pervasiveness and acceptance of a type of technology or business; and where the collection of those records, in totality, "provides a virtual current biography." *See DeJohn*, 403 A.2d at 1289-90.

Since the third-party doctrine is inapplicable, our Article I, Section 8 jurisprudence requires an analysis of whether engagement with Google is entirely volitional. Contrary to the OAJC's discussion, Article I, Section 8 protections do not hinge on the availability of other methods of engaging in an activity that do not involve third party access to an individual's information. *DeJohn* was not concerned with the availability of money orders or cash payments to conduct business. Instead, in the context of advancing electronic developments, the question was whether banking transactions had become so entrenched in society that engaging in those types of activities was not entirely volitional. Although alternatives were obviously available, the *DeJohn* Court did not consider alternatives and certainly, the failure to utilize available more anonymous alternatives did not render the use of banks entirely volitional. The OAJC does not employ the *DeJohn* Court's analysis that requires viewing the act of transferring information to a third party in the context of the modern operation of society. Instead, the OAJC employs a standard adopted from its interpretation of *Carpenter* that to maintain an expectation of privacy in information transferred to a third party, the transfer of the information must be totally involuntary. Thus, to the OAJC, the availability of alternative methods of conducting an activity (like the use of libraries or encyclopedias) that do not involve the transfer of information to a third party renders the activity involving the third party (the Google search) voluntary, divesting an individual of privacy in the Google search history. This constricted view of voluntariness has never been the law of Pennsylvania.

In my view, Google's compilation of boundless and unfathomable amounts of information to the exclusion of convenient access to the same information from other

sources renders the performance of searches to access that information not entirely volitional. Google is the ultimate research tool, as evident from the fact that the proper noun has become a verb: "I'll google it." It has rendered scarce hard copies of phone books, maps, encyclopedias, atlases, dictionaries, medical journals, law review articles, auto mechanic manuals, electric equipment repair manuals, etc.

In our technology-driven society, there is no meaningful choice but to use search engines to conveniently access information and the vast majority use Google to accomplish that task.[17] Their use is only voluntary to the extent it is voluntary to use a light switch to illuminate a room. Certainly, it is possible to use a flashlight or candles to accomplish the same goal—illumination—but it is not reasonable, convenient or efficient to do so in the daily tasks of modern society. For the vast majority of information, it is not realistic, or in some cases even possible, to use traditional source materials in hard copies like encyclopedias, phone books, atlases and specialized and generic dictionaries to access required or desired information. "It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting); *see also United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("[W]e should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society."). Our Article I, Section 8 jurisprudence demands a realistic consideration of the societal and personal consequences of forgoing the use of ubiquitous technology.

Because of the pervasiveness of the technology and the practical necessity of using it, the content being collected by Google "provides a virtual current biography[]" of its users. *See DeJohn*, 403 A.2d at 1289-90. Information inquiries reveal, among other things, the user's physical and mental health biography, political and religious views,

[17] *See* supra note 8.

medical concerns, travel plans, hobbies. The usefulness of the search results depends on the accuracy and specificity of the information used to perform the search, which means that a user paints a very personal biography when selecting terms to type and pressing enter.

Pennsylvanians must be able to search freely for information about matters idiosyncratically personal and those more broadly societal like candidates' views, political issues, religious doctrine and community causes. Given the strength of privacy rights under our Charter, it is inconceivable that the government can monitor and collect this information and the virtual personal biography developed by the mosaic of our search queries without first establishing probable cause and securing a warrant. The OAJC attempts to cabin the scope of its reasoning to "general, unprotected internet use." OAJC at 30. It highlights that "[t]here are a number of ways in which an internet user can hide or protect their browsing history[,]" such as using "private browsing mode … a private VPN, regularly delet[ing] his or her browsing history, opt[ing] out of data collection efforts by websites or applications, and limit[ing] or manag[ing] the 'Cookies' stored by websites." *Id*. at 22 n.81 (internal citation omitted). Where a user has taken such efforts, the OAJC suggests that "[t]he result may, in fact, differ[.]" *Id.* at 30. I question the suggestion that any attempt to disguise the identity of the inquirer would change the OAJC's conclusion that there is no expectation of privacy in information retained by search engine operators.[18] The predicate for its logic is that the internet search is entirely voluntary because of access to the information without the involvement of third parties. That

[18] Furthermore, I note that—aside from the Commonwealth's fleeting reference to Duck, Duck, Go as a more secure method of internet access than Google, Commonwealth's Brief at 29—no party raises the argument that utilizing alternative search methods would somehow change the third-party doctrine or the *DeJohn* analysis. Nor is there any record concerning the varying levels of online security articulated by the OAJC to support the alternatives it poses.

remains true despite the guises suggested by the OAJC. But even the guises suggested by the OAJC do not accomplish its perceived result. Deleting browsing histories and using a private browsing mode only hides the specific searches on the user's device but still enables search engines and internet service providers to retain records of such searches.[19] Utilizing a VPN may protect an internet user from hackers and bad actors in general but it is frightening to think that individuals must take steps to shield themselves from abuse of technology by the government as cautioned against in *DeJohn*.

Even if a Google user follows the OAJC's encouragement to disguise her identity by purchasing a VPN, this would have no impact on the OAJC's third-party doctrine analysis. While a VPN "masks" a user's IP address, *see* OAJC at 30 n.108, using a VPN does not change the fact that a user searching Google has shared information with Google, a third party. What the OAJC advocates for is essentially a way to prevent a search from being traceable to a specific user, but this does not alter the OAJC's rigid third-party framework. Moreover, the notion that using a VPN totally insulates an internet user from government detection is questionable because in certain circumstances the government may be able to ascertain the identity of an individual who utilizes a VPN.[20] This highlights the absurdity of the third-party doctrine and the OAJC's blind adherence to it. No matter the attempts at anonymity taken by an internet user, any search on any search engine involves the sharing of information with a third party. Even if an individual avoids all possible detection when sharing information with Google or a comparable third-

---

[19] *How to Clear Search History on Your Device*, BRAVE, https://brave.com/learn/how-to-delete-search-history/ (last visited Nov. 3, 2025).

[20] Drew Robb, *Can VPNs be Tracked by the Police?* TECH REPUBLIC (Apr. 10, 2025), https://www.techrepublic.com/article/can-vpns-be-tracked-by-police/. ("If the police can gain access to VPN connection logs, they may be able to find a user's actual IP address along with other information related to data usage and the times the user most commonly connects to the VPN. If the police obtain such broad access, they can generally put the pieces together to identify a specific user device and determine the user's identity.").

party search engine, the individual would be subject to the OAJC's third-party framework all the same as an individual who takes no precautions at all. Thus, the OAJC's alternative solutions, which are attempts to avoid detection and traceability, have no bearing on its application of the rigid third-party doctrine.[21]

Assuming for the sake of discussion the OAJC's position that users **might** have an expectation of privacy in search inquiries under some circumstances, the OAJC's musings are based on an unsupported notion that search engine users have the sophistication to unravel the intricacies of the technologies. This life vest is being thrown to users of those generations reared on internet usage or those with the time and insights to understand the inner workings of internet search engines, web browsers, ISPs and VPNs. No expectation of privacy with any meaning can depend on these variances. Fundamentally, I reject the OAJC's suggestion that one must take extra steps to vindicate what the Constitution already guarantees: protection of information stored by third parties where sharing the information in the first place is necessitated by participation in modern society.

Moreover, as to basic privacy expectations, 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. The OAJC counters that "the internet user at issue in this case is not the person sitting inside his home with the front door shut" but rather "more akin to a person sitting on the front porch of that house." OAJC at 31 n.109. The OAJC reasons that the privacy afforded by the home does not "protect what the person sitting on the front porch exposed to his neighbors." *Id.* The OAJC's analogy

[21] The other flaw with the OAJC's suggestion that alternate search methods may be protected is that, from the perspective of the government, it is impossible to know whether a user has taken extra steps to protect his or her privacy when the government first seeks search data from Google. Whether a warrant is required in the first instance cannot be contingent on what the government learns after the search data is already seized.

encapsulates its general underestimation of the role Google plays in society and the unique sense of security that individuals feel in sharing and searching for information on the machine-based search engine. The OAJC's front porch analogy is more comparable to a social media post where an individual shares information on an online platform to communicate a message to other human beings. Conversely, a Google search is a query posed to a mechanistic algorithm to either learn information, facilitate a task, or visit a website. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 647 (2011) (contrasting the sharing of information with human beings from the sharing of information with automated machines and proposing that courts "follow the lead of internet users themselves and choose to treat information disclosed only to automated systems as private[.]").

Google users share information with the inanimate search engine that they would not otherwise be comfortable sharing with another person, let alone a neighbor. Imagine an eighteen-year-old living with her parents who experiences an unplanned pregnancy. Not yet ready to discuss the matter with her parents, she takes her cell phone from her pocket and types "teen pregnancy resources" into Google. Or imagine a young man addicted to opioids at rock bottom. Ready to finally get clean, he picks his phone up from the kitchen table and types "help with opioid addiction" into Google. According to the OAJC, the sharing of these undeniably private circumstances with Google would be no different than had the young woman and man each stood on their front porches and shouted their searches for all to hear. The OAJC's solution: sign up for the subscription model of constitutional rights by purchasing a VPN, or you can earn your right to privacy by traveling to the library where, after scouring its shelves and paging through numerous books, you may be lucky to learn in hours what Google would have told you in seconds. What the OAJC refers to as "less convenient[,]" OAJC at 21 n.80, I call an undue burden

on the constitutional right to privacy that is out of touch with life in the twenty-first century and in contravention of our Article I, Section 8 jurisprudence. Accordingly, I conclude that society would find the expectation of privacy in internet searches to be objectively reasonable.[22]

Our finding that a constitutional privacy right exists may derive support from legislative enactments demonstrating that, as a matter of public policy, privacy overrides the societal interest in permitting the search. *Melilli*, 555 A.2d at 1258-59 & n.4 (citing *Beauford*, 475 A.2d at 790). We have acknowledged that the Pennsylvania Wiretap Act "is designed to safeguard individual privacy while also giving law enforcement authorities a tool to combat crime." *Commonwealth v. Fant*, 146 A.3d 1254, 1256 (Pa. 2016) (citing *Karoly v. Mancuso*, 65 A.3d 301, 303 (Pa. 2013)). The legislative effort "to limit [wiretapping] as much as possible to protect individual rights and give law enforcement the necessary tools[,]" *Beauford*, 475 A.2d at 790, is ubiquitous in the Act, and it does not apply only to traditional "wiretapping." The reasoning from *Beauford*, though written to address a different section of the Act, is equally applicable to 18 Pa.C.S. § 5743, which provides:

> (a) **Contents of communications in electronic storage.--** Investigative or law enforcement officers may require the disclosure by a provider of communication service of the contents of a communication which is in electronic storage in a communication system for:
>
> (1) One hundred eighty days or less only pursuant to a warrant issued under the Pennsylvania Rules of Criminal Procedure.

---

[22] Moreover, if the OAJC is correct that the government has unfettered access to this information, it would undoubtedly chill the exercise of First Amendment rights. I believe the question before us is answered fully by Article I, Section 8. There were apt analogies posited by amicus relating to the restrictions on searches on library computers and their reliance on First Amendment rights to protect search queries. These issues were not raised in the lower courts and not accepted for review by this Court.

> (2) More than 180 days by the means available under subsection (b).
>
> (b) Contents of communications in a remote computing service.--
>
> (1) Investigative or law enforcement officers may require a provider of remote computing service to disclose the contents of any communication to which this paragraph is made applicable by paragraph (2):
>
> (i) without required notice to the subscriber or customer if the investigative or law enforcement officer obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure; or
>
> (ii) with prior notice from the investigative or law enforcement officer to the subscriber or customer if the investigative or law enforcement officer:
>
> (A) uses an administrative subpoena authorized by a statute or a grand jury subpoena; or
>
> (B) obtains a court order for the disclosure under subsection (d); except that delayed notice may be given pursuant to section 5745 (relating to delayed notice).
>
> (2) Paragraph (1) is applicable with respect to a communication which is held or maintained on that service:
>
> (i) On behalf of and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the remote computing service.
>
> (ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

18 Pa.C.S. § 5743(a)-(b).[23] As with the warrant requirement discussed in *Beauford*, the Legislature declared its intention that information held by providers like Google "does not

[23] Under either subsection (a) or (b), a warrant is required unless law enforcement provides notice to the subscriber or customer.

thereby enter the public domain, or the field of scrutiny open to the police." *Beauford*, 475 A.2d at 790. It did so in certain terms by requiring law enforcement to secure a warrant to require Google to turn over the contents of a communication within electronic storage for less than 180 days.[24] 18 Pa.C.S. § 5743(a)(1). For over thirty-six years, the

---

[24] In addressing this issue, the Amici, the Office of the Attorney General and the Pennsylvania District Attorneys Association (collectively "OAG"), suggest that Section 5743 "arguably requir[ed police] to obtain a warrant in these circumstances regardless of whether one is constitutionally required." OAG's Brief at 10-11. Chief Justice Todd relies on this suggestion as the basis for avoiding this constitutional issue in this case. Concurring Op. at 2, 6 n.6 (Todd, C.J.).

The original 1988-version of Section 5743(a) appears to have been copied (almost verbatim) from the 1986-version of Section 2703(a) of the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703(a). Both applied to law enforcement requests requiring disclosure by "a provider of electronic communication service of the contents of an electronic communication which is in electronic storage in an electronic communication system[,]" and both required warrants for requests for contents of such communications in storage for one hundred and eighty days or less. 18 Pa.C.S. § 5743(a) (ver. 1988), 18 U.S.C. § 2703(a) (ver. 1986) (differing only by addition of a comma and use of "that" instead of "which").

Google is uniformly treated as a provider of communication service under Section 2703 by federal courts. *See, e.g.*, *Matter of Search of Information Associated with One Email Account*, 677 F.Supp.3d 580 (E.D.Tex. 2023) (explaining that Section 2703 gave provider, i.e., Google, the right to move to quash warrant, but not the customer); *In re Search of Records, Information, and Data Associated with 14 Email Addresses*, 438 F.Supp.3d 771, 775 (E.D. Mich. 2020); *Frank v. Gaos*, 586 U.S. 485 (2019) (per curiam) (in cy pres litigation Google agreed to settlement resolving claims based on violation of the Electronic Communications Privacy Act by Google); *see also In re Google Assistant Privacy Litigation*, 457 F.Supp.3d 797, 822-23 (N.D. Cal. 2020) (addressing claim of voluntary disclosure of customer communications or records and treating Google as an entity providing electronic communication services under 18 U.S.C. 2702(a)); *Calhoun v. Google, LLC*, 526 F.Supp.3d 605, 626 (N.D. Cal. 2021) (rejecting the plaintiff's argument that Chrome was the entity providing the electronic communication service because "the 'person or entity providing the electronic communication service is Google[]'" under 18 U.S.C. § 2701(c)(1)). Given that Section 5743 largely tracks and derives from Section 2703, Google is equally a provider subject to the warrant requirement established in Section 5743.

Section 5743 is stronger and clearer than some other sections of the Act, which are also read to require a warrant and protect important privacy interests, but do not include the explicit warrant requirement articulated in Section 5743. *Compare* 18 Pa.C.S. § 5743 (continued…)

General Assembly has not modified this requirement. Given that the Wiretap Act requires the government to obtain a warrant to access a Google user's search information, Google users have an unqualified expectation in this jurisdiction that such information will be protected from indiscriminate government monitoring. This legislation is an unambiguous statement that the legislature recognizes that this expectation of privacy is objectively reasonable.

Google's Privacy Policy in this case supports the conclusion that users have an expectation of privacy in their searches. According to Google's Privacy Policy, Google "share[s] personal information with companies, organizations or individuals outside of Google only when [it] ha[s] your consent to do so." Google Privacy Policy, at 4. Further, "[f]or legal reasons," Google "will share personal information with companies, organizations, or individuals outside of Google if [it] ha[s] a good-faith belief that access, use, preservation or disclosure of information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request[]" or to "to protect against harm to the rights, property or safety of Google, [its] users or the public as required or permitted by law." *Id*. Under the heading of "**Information security**" Google's Privacy Policy indicates that it "work[s] hard to protect Google and [its] users from unauthorized access to … information [it] hold[s]." *Id*. Google's Privacy Policy clearly demonstrates that this information does not "enter the public domain, or the field of scrutiny open to the police." *Beauford*, 475 A.2d at 790.

The OAJC concludes from Google's Privacy Policy that a user "is aware (at least constructively) that Google collects a significant amount of data and will provide that data

---

(a)(1) (providing law enforcement may require this type of disclosure "only pursuant to a warrant issued under the Pennsylvania Rules of Criminal Procedure") *with* 18 Pa.C.S. § 5773 (a) (providing requirement of a court order supported by probable cause, but not warrant, for use of certain devices).

to law enforcement in response to an enforceable search warrant." OAJC at 23. While the OAJC recites the language of the Privacy Policy, it fails to grapple with the meaning of the words, i.e., the user can expect that her privacy will be maintained from government access unless it is required to reveal information based on an enforceable warrant. The OAJC diminishes the express language of the Policy to claim that "the standards [Google] imposes upon itself before providing that information to investigators[] [are] irrelevant." *Id*. at 24. The question is: irrelevant to what? It is certainly not irrelevant to the user's expectation of privacy in the shared information.

To the OAJC, what matters is that Google "will collect and store that information." *Id*. However, banks also collect and store information, as do telephone companies, (to wit, pen registers). These facts are integral to *DeJohn* and *Melilli*.

The OAJC's analysis cannot be squared with the plain language of Google's Privacy Policy. Google informs its users in the Privacy Policy that it will only disclose information to the government when "reasonably necessary" to "meet any applicable law, regulation, legal process or **enforceable** government request." Google's Privacy Policy at 4 (emphasis added). If the information is not protected as private, then why would Google purport to require a legally enforceable request? And why would it reassure users about information security? In light of the agreement between Google and the user, this is not a case of "general, unprotected internet use." OAJC at 30. Rather, the terms of Google's Privacy Policy inform that a reasonable Google user would expect that his search history would not be shared with the government without a search warrant. What better indicator could there be to find that a user has an expectation of privacy in that information?

This rationale is implicitly supported by our decision in *Commonwealth v. Dunkins*, 263 A.3d 247 (Pa. 2021), where we determined that a college student had no expectation

of privacy in campus witness internet (WiFi) connection records based on the college's computing resources policy stating as much. *Dunkins*, 263 A.3d at 250. The policy in *Dunkins* provided that "users cannot and should not have any expectation of privacy with regard to any data … created or stored on computers within or connected to the institution's network." *Id.* (internal citation omitted). The *Dunkins* Court concluded that the student "relinquished any purported expectation of privacy in the WiFi connection records" because he "assent[ed] to the Computing Resources Policy and logg[ed] on to the [campus] WiFi network on his cell phone thereafter[.]" *Id.* at 255. If an internet user can waive his expectation of privacy based on the terms of a privacy policy, the terms of a privacy policy—such as Google's in this case—must also reinforce a user's expectation of privacy in his internet searches.

Aside from its misreading of the Privacy Policy, the OAJC's analysis smacks of the unexamined notion of voluntariness at the heart of the third-party doctrine, a doctrine that this Court has repeatedly rejected. The only foundation for the OAJC's position—that by sharing information with Google, a user risks that his information will be shared with other companies and the public at large and therefore Kurtz must accept that his information will be available to law enforcement—is not consistent with our Article I, Section 8 jurisprudence. Google does not purport to indiscriminately share users' personal information. Based on Google's Privacy Policy, Kurtz had no reason to expect that his search queries would be made generally available to the public or freely shared with law enforcement. Google's use of information for its purposes, and its disclosure of non-personally identifiable information to private companies for marketing purposes is no more antithetical to privacy than it was with regard to CSLI in *Pacheco* and *Carpenter*. *Carpenter*, 585 U.S. at 301 (finding a reasonable expectation in CSLI notwithstanding that the information is collected and stored for business purposes, including by being sold

(anonymized) to private data brokers). "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." *Smith,* 442 U.S. at 749 (Marshall, J., dissenting). It is undisputed that Google, as a private for-profit enterprise utilizes information obtained from users for marketing purposes. Google users agree to take part in that business model in exchange for access to boundless troves of information about almost any imaginable subject, thus gaining access to knowledge that otherwise might not be attainable. That is the bargained-for exchange cabined by the express terms of the Google Privacy Policy which integrates the warrant requirement contained in the Wiretap Act.

Now is not the time to retreat from *DeJohn*. It predicted the dangers of government abuse of technological advances that become embedded in contemporary society. The utilization of Google and other internet search engines to search for information is at least as ubiquitous as the utilization of banking institutions were when *DeJohn* was decided in 1979. Most younger generations do not remember a time when Google was not the go-to source of any and all information. Many other alternatives to access the same information not involving third parties no longer exist. If they do exist, they are likely not readily obtainable by average citizens. It is unfathomable that the search for information bears the price tag of the loss of privacy from the government in the mere request for the information.

An individual has an expectation that the information will be free from government surveillance because the utilization of the technology for gaining information is a requirement for participation in contemporary society. The Google Privacy Policy which cabins the sharing of the information reflects this expectation, and legislation prohibiting unchecked government access to it clearly demonstrates society's recognition that the

expectation is reasonable. Our Article I, Section 8 jurisprudence demands that we recognize this reasonable expectation of privacy.

III. Probable Cause[25]

Because Kurtz has a reasonable expectation of privacy in his Google search queries implicating the warrant requirement, it was incumbent upon the Commonwealth to demonstrate probable cause to obtain a keyword search warrant. The keyword search warrant, being devoid of individualized suspicion targeting any identified person's Google records, fails the test for probable cause by falling substantially short of demonstrating a nexus between the location of the search (Google's database) and the crime under investigation. Consequently, the Superior Court erred when it failed to reverse the suppression court's decision not to grant Kurtz's motion to suppress.

Kurtz asserts that law enforcement failed to establish probable cause to support the warrant because the affidavit of probable cause "was merely speculative[,] [and it] was not supported by facts or circumstances that would have caused an individual of reasonable caution to believe that Google, Inc. was involved in any way in the commission of the crimes." Kurtz's Brief at 35. In support, he walks through recent case law regarding probable cause, distinguishing the present case from *Commonwealth v. Johnson*, 42 A.3d 1017 (Pa. 2012), where police observations of the crime scene where a young child was beaten, witness statements, and an inculpatory statement by Johnson were enough to establish probable cause. *Id*. at 35-36. He contrasts *Johnson* with *Commonwealth v. Jacoby*, 170 A.3d 1065 (Pa. 2017), where we held that a warrant lacked probable cause because it was based on general assumptions rather than concrete facts, arguing that the circumstances of this case are more akin to those in *Jacoby* in the prevalence of

[25] For this issue, Kurtz does not meaningfully distinguish between the Fourth Amendment and Article I, Section 8.

assumptions in the affidavit of probable cause. Finally, he distinguishes *Commonwealth v. Jones*, 988 A.2d 649 (Pa. 2010), where this Court held that an affidavit requesting a search warrant for a college dormitory sufficiently established probable cause. Kurtz's Brief at 39-41.

The Commonwealth presents only a cursory analysis of the issue, relying on case law to establish the standard of review. It cites *Jones* for the proposition that a reviewing court must only "examine[] whether a substantial basis exists for the issuing authority's finding of probable cause[,]" and that the issuing authority's "determination is entitled to deference[,]" but otherwise draws no parallels between that case and this one. Commonwealth's Brief at 41 (citing *Jones*, 988 A.2d at 655). The Commonwealth concedes that there is no direct evidence that Google was used but believes that the circumstances and nature of the crime, considered together with the ubiquity of Google, "provide a fair probability that Google was used, and evidence would be found." *Id*. at 42-43.

In my view, none of the cases cited by the parties provide focused guidance regarding keyword search warrants beyond general principles applicable to all search warrants. *Johnson* involved an affidavit of probable cause providing ample evidence that justified the search of a physical location where a fatal assault occurred. *See Johnson*, 42 A.3d at 1031-32 (indicating that the affidavit of probable cause stated that "victim had been injured, the injury occurred at the residence, mother indicated [Johnson] assaulted victim, there were conflicting accounts of how victim had been injured, and there was likely to be evidence pertaining to the injury in the residence"). In *Jacoby*, police obtained a warrant to search a suspect's home for a firearm more than a year after he committed a murder at a different location. *Jacoby*, 170 A.3d at 1073-74. In *Jacoby*, we rejected the notion that probable cause existed to search Jacoby's home—fifteen months after the

murder—merely because "probable cause existed to believe that he had committed the murder, with a weapon of the same caliber as one that he owned, and then drove in the general direction of his home" after the killing. *Id*. at 1084. The nexus between the crime and the physical location to be searched was simply too remote both temporally and geographically to establish probable cause for the search. *Id.* at 1085. Here, there was no physical location searched, no direct link to Google's databases beyond bare assumptions about the ubiquity of Google searches, and police did not have any suspect in mind when they obtained the keyword search warrant.

Jones involved a specific physical location—the dorm room Jones shared with the victim—but the affidavit of probable cause did not target Jones as a suspect. Kurtz distinguishes *Jones* on the basis that the affidavit of probable cause in that case contained substantially more specific facts demonstrating a nexus between the crime and the location searched. Kurtz's Brief at 39-40.[26] In *Jones*, police responded to reports of a shooting on campus and found the deceased victim riddled with bullets. A witness observed a man running from the scene of the shooting and provided a description to police that matched Jones. A set of keys found on the victim suggested he was a Widener student, a fact corroborated by university officials who provided a photo from their student

[26] The Commonwealth quotes *Jones* at length for our standard of review of probable cause determinations, but it makes no discernable effort to contest Kurtz's assertion that *Jones* is factually distinguishable. *See* Commonwealth's Brief at 40-41. The OAG insinuates that Kurtz challenges the keyword warrant because it is investigatory, *see* OAG's Brief at 20, but that mispresents Kurtz's argument. Nor does Kurtz assert, as Amici claim, that a search warrant must always target a specifically identified person. *Id*. at 21. Kurtz merely describes the keyword search warrant as investigatory and then distinguishes *Jones* as demonstrative of circumstances where a warrant that targets a particular location but lacks individualized suspicion targeting a person is permitted. Kurtz's Brief at 34; 39-40. Kurtz does not assert that the keyword search warrant is invalid because it was investigatory in nature. He also does not claim that a search warrant can never issue without identifying a specific person as the target of an investigation; he simply notes that no person was identified in the affidavit of probable cause as one factor contributing to the absence of probable cause. *Id*. at 40-41.

records. During the investigation, Jones told police that the victim had left their room the night before after speaking on his cell phone and never returned. *Jones*, 988 A.2d at 651.

The magistrate issued a warrant to search the room that Jones shared with the victim based on an affidavit of probable cause setting forth the facts above. The search produced the victim's bloody cellphone and other evidence used to convict Jones after the trial court denied Jones' suppression motion. The Superior Court reversed, holding that probable cause was lacking to justify a search for the particular evidence identified in the search warrant (drug-related evidence), and because there was no need to verify the victim's identity as police had ostensibly identified him before the search occurred. We reversed the Superior Court, holding that "[t]he affidavit of probable cause reasonably identified what was probably the last residence of the victim, within which there was a fair probability that the police would find evidence of the murder that had occurred nearby. Moreover, access to the dormitory room was required to obtain conclusive identification of the victim." *Id*. at 656-57.

The police in *Jones* demonstrated an obvious link between the target of the search and the criminal activity in question for purposes of probable cause. The victim's dorm room was the last location where he had been seen before he was found murdered just a few blocks away, keys to that room were found on his body, and his cellphone was missing—the cellphone that Jones told police that the victim had used inside the dorm room shortly before he was killed. We ultimately rejected Jones' arguments that a warrant cannot serve a purely investigative purpose under both the federal and state constitutions. *Id*. at 657.

However, Kurtz does not challenge whether a keyword warrant can serve an investigatory purpose. The issue here is the absence of individualized suspicion targeting the location to be searched, and the facts of this case are distinguishable from *Jones* in

that regard. Police in *Jones* searched one dorm room based on several facts showing a nexus between the victim's murder and his nearby dorm room where he was last seen alive. Here, police asked Google to sift through countless different users' data for keywords based only on a hunch that the perpetrator had conducted a Google search using those keywords. Thus, while Kurtz is correct that *Jones* does not support that Trooper Follmer's affidavit established probable cause, it also has limited instructive value because it involved the search of a discrete physical location with obvious links to the murder under investigation.

By contrast, the instant matter concerns the application of established constitutional standards for probable cause to technological advances that provide new and untested fact patterns for Fourth Amendment analysis. None of the cases discussed by the parties involved the search of vast electronic databases in the absence of individualized suspicion. Accordingly, I preface my analysis by examining the evolution of probable cause jurisprudence as it pertains to searches conducted absent individualized suspicion.

The "Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and of the writs of assistance used in the Colonies." *Steagald v. United States*, 451 U.S. 204, 220 (1981).[27]

> The general warrant specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. Similarly, the writs of assistance used in the Colonies noted only the object of the search—any uncustomed goods—and thus left customs officials completely free to search any place where they believed such goods might be. The central objectionable feature of both warrants was that they provided no judicial

[27] *See also Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (stating that the Fourth Amendment "was a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies").

> check on the determination of the executing officials that the evidence available justified an intrusion into any particular home.

Id.

In order to protect "the sanctity of a man's home and the privacies of life" in the wake of these abuses of government authority in Colonial America, the Fourth Amendment required warrants to describe "the place to be searched, and the persons or things to be seized[.]" *Hayden*, 387 U.S. at 301 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886) and *McDonald v. United States*, 335 U.S. 451, 455 (1948)); *accord Jacoby*, 170 A.3d at 1085 ("The architects of our Constitutions rejected general searches, and instead charged police officers with demonstrating **specific and articulable facts** to establish probable cause that a **particular** person committed a **particular** crime and that evidence of that crime would be found in a **particular** place.") (emphasis added). Today, however, the "modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). Companies like Google magnify this problem and the importance of particularity because the private inquiries of billions of users are digitally stored and thereby left accessible to law enforcement with warrant in hand.

The founders could not have conceived of a world of pocket-sized supercomputers that are interconnected in a global communication network that contains the full extent of human knowledge (or close to it). To say that they did not envision the case before us today risks only understatement of the revolutionary changes in technology that have occurred in the last two and a half centuries. Rather than searches of illegal goods or incriminating papers in warehouses or private homes, we are now concerned with

searches of electronic databases that store the search inquiries of **billions** of people, and hundreds of millions in the United States, most of whom assume that those searches will remain private and not subject to fishing expeditions by law enforcement as established above. While the technology involved today is radically different, and direct comparisons are imperfect, there are some analogies to be drawn to the targets of the founders' concerns— general warrants and writs of assistance.

Here, the police acted on a hunch that the victim's residence was the target of a Google search by the unknown perpetrator and secured a warrant on that basis. This is conceptually no different than predicting contraband will likely be found through searches of every warehouse adjacent to the docks in the years before the Fourth Amendment was adopted. The general warrants and writs of assistance issued in the pre-revolutionary era were problematic, in part, because they were issued absent any individualized suspicion of wrongdoing, even though they were almost certain to produce evidence of wrongdoing given the scope of searches that they authorized. Similarly, the keyword search warrant in this case was issued on the pretext that it was likely to produce evidence of the crime under investigation even though the affidavit of probable cause failed to show any individualized suspicion regarding the location to be searched, i.e., Google's stored user information.

This Court should be cautious not to substantially rely on the probability that evidence of criminality will be discovered when conducting a probable cause analysis for two reasons. First, as a practical matter, the measurement of that probability will always be distorted by hindsight given that fruitless searches will never be litigated at a suppression hearing. Reasonableness is the touchtone of Fourth Amendment

jurisprudence,[28] and one of the core purposes of the warrant requirement "is to prevent hindsight from coloring the evaluation of the reasonableness of a search or seizure." *United States v. Martinez-Fuerte*, 428 U.S. 543, 565 (1976). In every case in which we address suppression, the Commonwealth uncovered evidence it deemed important enough to use at a criminal trial. Thus, we must carefully guard against hindsight bias that would have us believe the Commonwealth's success was predictable at the time the warrant was sought.[29] Sometimes a police officer's hunch proves true, but that does not elevate a hunch to the level of probable cause.

Second, the scope of a warrant's reach can be so broad as to make the discovery of incriminating evidence inevitable, especially in the absence of individualized suspicion. For example, we can predict with confidence that a warrant to search every home in Pennsylvania for a certain type of contraband, packaged in a particular way, will produce evidence of a crime. This is precisely what general warrants and writs of assistance accomplished, as the discovery of contraband was inevitable when searching every arriving ship or warehouse in Boston Harbor on the reasonable belief that the targeted contraband was arriving by sea. The lesson is that a warrant may provide a plethora of specifics—and portend a high probability of discovery of evidence of criminality—but nonetheless be defective for lack of individualized suspicion in the person or location to

[28] The Fourth Amendment's "central requirement" is "one of reasonableness." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (citing *Texas v. Brown*, 460 U.S. 730, 739 (1983)).

[29] Consequently, the Commonwealth is totally incorrect and dangerously illogical in asserting that the "fact that the search warrant yielded probative evidence confirms probable cause did exist to believe such evidence could be found." Commonwealth's Brief at 43.

be searched.[30] To hold otherwise would be to invite the return of general warrants and writs of assistance.

Analysis

Our review of the denial of suppression is limited to whether the suppression court's factual findings are supported by the record and whether the legal conclusions are free of error. *Jones*, 988 A.2d at 654.[31] Our review of the legality of search warrants is focused on whether the issuing authority possessed a "substantial basis" to find probable cause. *Johnson*, 42 A.3d at 1031. "Probable cause exists where the facts and circumstances within the affiant's knowledge and of which he has reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that a search should be conducted." *Commonwealth v. Thomas*, 292 A.2d 352, 357 (Pa. 1972). In reviewing warrants, we must afford some deference to the magistrate's determination when reasonable minds might differ on whether a particular affidavit establishes probable cause. *See Jones*, 988 A.2d at 655-56.

"Deference to the magistrate, however, is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Id*. at 915 (quoting *Illinois v. Gates*, 462 U.S. 213, 239,

---

[30] "[T]he general rule is that probable cause must be predicated upon individualized suspicion, and that searches conducted without such suspicion ordinarily are deemed unreasonable" even though "[n]either the Fourth Amendment nor Article I, Section 8 of the Pennsylvania Constitution explicitly requires individualized suspicion." *Jacoby*, 170 A.3d at 1084; *see also Commonwealth v. Mistler*, 912 A.2d 1265, 1271 (Pa. 2006) (stating "the Fourth Amendment generally requires the presence of individualized suspicion").

[31] In this regard, "we may consider only the evidence of the Commonwealth and so much of the evidence for the defense as remains uncontradicted when read in the context of the record as a whole[;]" when the suppression court's "factual findings are supported by the record, we are bound by these findings and may reverse only if the court's legal conclusions are erroneous." *Jones*, 988 A.2d at 654.

(1983)). Additionally, as a majority of Justices articulated in *Jones* through the concurrences of then-Chief Justice Castille and then-Justice Todd, when facts and credibility are not in dispute, our review of pure legal questions concerning the existence of probable cause is plenary. *See Jones*, 988 A.2d at 660 (Castille, C.J., concurring) ("When the question is a purely legal one (such as the question of whether an agreed-upon set of facts and circumstances establishes probable cause), there is no jurisprudential reason for a reviewing court to defer to the judgment of any entity below."); *id.* at 664 (Todd, J., concurring) (stating "appellate review of the magistrate's legal determination of probable cause, as with appellate review of all legal questions, remains plenary"). In that vein, "wholly conclusory" sworn statements about what the affiant believes to be true, even if the affiant attests that his conclusions are based on reliable information from credible sources, do not provide a substantial basis to find probable cause. *Gates*, 462 U.S. at 239 (citing *Nathanson v. United States*, 290 U.S. 41 (1933) (holding insufficient a customs agent's belief about the location of contraband liquor) and *Aguilar v. Texas*, 378 U.S. 108 (1964) (holding insufficient an officer's sworn statement that he had reliable information from a credible source regarding the presence of heroin at a particular home)).

Under our Rules of Criminal Procedure, a search warrant must be supported by at least one signed and sworn written affidavit. *See* Pa.R.Crim.P. 203(B), 206. "The issuing authority, in determining whether probable cause has been established, may not consider any evidence outside the affidavits." Pa.R.Crim.P. 203(B). Likewise, at a suppression hearing, "no evidence shall be admissible to establish probable cause other than the affidavits provided for in paragraph (B)." Pa.R.Crim.P. 203(D). "Each search warrant" shall, inter alia, "identify specifically the property or person to be seized" and "name or describe with particularity the person or place to be searched[.]" Pa.R.Crim.P. 205(a). A

search warrant "may authorize the seizure of electronic storage media or of electronically stored information" and, unless "otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Pa.R.Crim.P. 205(b).

Although the totality of the circumstances test applies to assessments of probable cause, there are some guideposts pertinent to the instant case. The Fourth Amendment strongly favors the finding of individualized suspicion, and so further discussion of that requirement is in order. As we stated in *Jacoby*, the requirement of individualized suspicion is the general rule subject to a few, well-defined exceptions. *Jacoby*, 170 A.3d at 1084. As we recounted in *Mistler*, the United States Supreme Court has identified four exceptions to the individual suspicion requirement that permits suspension of the warrant requirement altogether: 1) drug tests of student athletes and certain employees; 2) administrative searches of heavily regulated businesses; 3) border patrol checkpoint searches; and 4) sobriety checkpoints. *See Mistler*, 912 A.2d at 1271 (compiling cases). This Court has similarly upheld suspicionless searches at vehicle checkpoints for the detection of unlicensed drivers and dangerous vehicles, and for weapon and some drug searches in public schools. *Id*. at 1271-72 (compiling cases).

The common theme among these exceptions to the general requirement of individualized suspicion, and the warrant requirement itself, is that the sanctioned searches were "designed to serve 'special needs, beyond the normal need for law enforcement.'" *Id*. at 1271 (quoting *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000)). As noted in *City of Indianapolis*, exceptions to the general rule typically involve higher purposes like border control or roadway safety, not just the omnipresent general interest in the enforcement of criminal laws. *City of Indianapolis*, 531 U.S. at 41. But the instant matter does not involve broader public policy concerns or special needs beyond a general interest in enforcing criminal laws. To the contrary, this case involves the

investigation of a specific criminal episode and is, thus, quintessentially a matter involving "ordinary criminal wrongdoing" for which individualized suspicion is required to establish probable cause for purposes of obtaining a search warrant. *City of Indianapolis*, 531 U.S. at 42. Thus, those cases do not provide an analytical framework to analyze the matter before us.

Consideration of another category of cases provides a more analogous context to keyword search warrants—those cases involving all-persons-present warrants ("APP warrants"). In *Ybarra v. Illinois*, 444 U.S. 85 (1979),[32] the United States Supreme Court specifically reserved for another day the constitutionality of "situations where the warrant itself authorizes the search of unnamed persons in a place and is supported by probable cause to believe that persons who will be in the place at the time of the search will be in possession of illegal drugs." *Id*. at 92 n.4. On the one occasion this Court addressed APP warrants, we split evenly and affirmed, by default, the use of APP warrants in the two cases under review. *See Commonwealth v. Gilliam*, 560 A.2d 140 (Pa. 1989). In *Gilliam*, we considered the Superior Court's approval of APP warrants in both *Commonwealth v. Heidelberg*, 535 A.2d 611 (Pa. Super. 1987), and *Commonwealth v. Gilliam*, 538 A.2d 938 (Pa. Super. 1987) (non-precedential decision).

---

[32] In *Ybarra*, the High Court confronted a scenario where police obtained a search warrant for a tavern based on specific information that a heroin sale would occur on a certain date. When police arrived at the designated time and location, they announced to the patrons that they were going to pat down everyone for weapons. Police detected a cigarette pack in Ybarra's pocket, searched it, and discovered heroin packets. Ybarra's suppression motion was denied, and the state appellate court affirmed under the theory that because the otherwise-valid warrant targeted a one-room bar, depriving the police of the ability to search individuals present who could easily conceal the heroin on their person would thwart the purpose of the warrant. The *Ybarra* court reversed, rejecting the state's theory that the Fourth Amendment permitted "evidence searches of persons who, at the commencement of the search, are on 'compact' premises subject to a search warrant [and] where the police have a 'reasonable belief' that such persons 'are connected with' drug trafficking and 'may be concealing or carrying away the contraband.'" *Ybarra*, 444 U.S. at 94.

Writing for himself and two other Justices, Justice Flaherty agreed with the Superior Court that APP warrants are disfavored but not per se invalid. *Gilliam*, 560 A.2d at 142. Critically, he wrote that rather than barring APP warrants altogether, "the better approach is to examine each case to see whether, **under strict scrutiny**, the affidavit in support of the warrant makes out a sufficient nexus between the physical location to be searched and the likelihood that every person present at that location is involved in the criminal activity at issue." *Id*. at 142-43 (emphasis in original).[33] However, it is important to note that the United States Supreme Court has never decided the question posed hypothetically in *Ybarra*—whether APP warrants are constitutional **even if** supported by probable cause to believe that every **unnamed** person found at the targeted location is engaged in criminal activity.

While the standard articulated by Justice Flaherty in *Gilliam* was not officially adopted by this Court, it represents a majority view among courts that have approved APP warrants (without the reference to strict scrutiny). *See, e.g.*, *United States v. Abbott*, 574 F.3d 203, 212 (3d Cir. 2009) (holding "that a warrant may authorize the search of all persons present if there is probable cause to believe that a premises is dedicated to criminal activity");[34] *Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (holding "an [APP] warrant can pass constitutional muster if the affidavit and information provided to the magistrate supply enough detailed information to establish probable cause to believe that

---

[33] Justice Flaherty would have reversed the orders affirming the APP warrants under the facts. *Gilliam*, 560 A.2d at 143 ("It was certainly reasonable to search the premises, but it was not reasonable to search unnamed persons who might be found on the premises merely because drugs had been recently sold and stored there. It is not enough that persons present might be involved. In order for an [APP warrant] to be valid under Article I, Section 8 of the Pennsylvania Constitution, it must be shown that all persons present were probably involved in the illegal activity.").

[34] This "den of thieves" theory appears to be the lowest bar set by courts that have approved APP warrants.

all persons on the premises at the time of the search are involved in the criminal activity"); *Marks v. Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996) (recognizing that an APP warrant "may only be obtained when there is reason to believe that all those present will be participants in the suspected criminal activity;" declining to generally approve of the "den of thieves" theory, but opining it might be viable for narrowly-defined locations like a "crack house" or a "barn used as a methamphetamine lab"); *State v. De Simone*, 288 A.2d 849, 850 (N.J. 1972) ("So long as there is good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant, presence becomes the descriptive fact satisfying the aim of the Fourth Amendment."); *People v. Nieves*, 330 N.E.2d 26, 34 (N.Y. 1975) (condoning APP warrants only where "the facts before the issuing Judge at the time of the warrant application, and reasonable inferences from those facts, ... establish probable cause to believe that the premises are confined to ongoing illegal activity and that every person within the orbit of the search possesses the articles sought"); *State v. Vandiver*, 891 P.2d 350, 357 (Kan. 1995) (same); *State v. Prior*, 617 N.W.2d 260, 263-64 (Iowa 2000) (stating that an APP warrant must "be supported by facts showing a substantial probability that the authorized invasions of privacy will be justified by the discovery of the items sought from all persons present when the warrant is executed") (internal quotation marks and citations omitted).[35]

---

[35] A minority of jurisdictions have rejected APP warrants outright, albeit not always on constitutional grounds. *See, e.g.*, *Beeler v. State*, 677 P.2d 653, 656 (Okla. Crim. App. 1984) (holding where "probable cause is the standard, a search or seizure of a person must be supported by probable cause particularized with respect to that person" and that "requirement may not be undercut by pointing to the coincidental existence of probable cause to search or seize another or to search the premises where the person may happen to be"); *State v. Reid*, 872 P.2d 416, 419 (Or. 1994) (holding an APP warrant "failed to satisfy" Oregon's statutory requirements because "the affidavit did not demonstrate probable cause to believe that all 'persons present' on the premises would be associated with the criminal activity taking place there"); *State v. Holmes*, 525 S.E.2d 698, 700 (Ga. App. 1999) (stating the "inclusion of language in the warrant authorizing the search of 'any persons present' on the premises does not broaden the powers of the searching (continued…)

The unifying principle of the cases permitting APP warrants is that there must be probable cause to search every individual likely to be present when the warrant is executed. Even under the "den of thieves" theory adopted in *Abbott*, it must be shown that the location to be searched is primarily used for illegal purposes, such that anyone present is likely to be involved in the criminal activity that provided the impetus for the warrant. As discussed below, neither circumstance is present in this case.

Affidavit of Probable Cause

Here, there was only one affidavit filed with the search warrant application. Therein, Trooper Joel Follmer of the Pennsylvania State Police stated his belief as to why probable cause existed to search Google's database for IP addresses associated with keyword search inquiries relating to the victim's name and address occurring between July 13 and July 20 of 2016—a timeframe representing the week leading up to the crime under investigation.[36] The affidavit first provided a brief description of the offense.

Trooper Follmer recounted that he first met with the victim at the emergency room on July 20, 2016. Affidavit of Probable Cause, 9/14/2016, at 1. The victim told Trooper Follmer that, around 2 a.m. that morning, she twice awoke to the sound of her dogs barking. *Id*. On the first occasion, she investigated but soon returned to bed after not seeing anything out of the ordinary. *Id*. On the second occasion, she again searched her home and was soon assaulted by an unknown male who quickly restrained her with a zip-tie, cloth gag, and blindfold. *Id*. The victim lost consciousness as she struggled with her assailant; when she regained consciousness, she was being dragged by her feet to a

---

authorities beyond the limited terms" of the Georgia statute governing the detention and search of persons on premises).

[36] More specifically, Trooper Follmer requested Google's historical records of Google search and Google image search queries for the victim's name, and Google search and Google Maps search queries for the victim's address, occurring between July 13 and July 20 of 2016. Application for Search Warrant, Attachment A; supra note 6.

vehicle. *Id*. The assailant loaded her into a vehicle and drove for approximately forty-five minutes. *Id*. Before stopping, the victim noticed that they were driving along a gravel road or driveway. *Id*. The assailant then removed her from the vehicle and took her into a nearby structure where he raped her. *Id*. Following the rape, the victim was returned to a cornfield located within a mile of her home, where the assailant removed her restraints and instructed her to walk into the cornfield and to not turn around. *Id*. Approximately fifteen minutes after the assailant fled, the victim walked to a nearby residence where police were summoned. *Id*.

Following this recitation of facts, Trooper Follmer stated:

> Based off the assessment of the incident, it is believed that the Actor was very familiar with the VICTIM and the VICTIM was not randomly targeted. The VICTIM'S residence was also not randomly targeted. The VICTIM lives in a very small rural development outside the borough of Milton, PA and the whereabouts are likely unknown by most. Furthermore, it is believed that the Actor knew that the VICTIM'S husband was not home at the time of the entry into the residence. It is also believed that the Actor may have spent some time stalking the VICTIM and her husband's schedule as well as their whereabouts. Most sexual offenders of this magnitude are predominately fantasy driven, which could have occurred over a lengthy period of time. The VICTIM moved into the area in July 2015. It is believed that the Actor may have fantasized about the VICTIM, after seeing or becoming aware of her, and it is likely that he followed her back to her address. Furthermore, it is believed that the Actor also researched the VICTIM'S address and/or VICTIM utilizing the internet or search engine similar to the searches provided by Google Inc.

Id.

None of these "beliefs" amounts to probable cause to conduct a search of all Google search engine users for individuals who used keywords related to the victim and/or her address. Instead, Trooper Follmer offered the issuing authority a series of unsupported hunches lacking individualized suspicion targeting Kurtz and bereft of any articulated nexus between the described offense and Google's database of stored search

inquiries. The bottom line is that Trooper Follmer sought a warrant to search Google's vast database because he believed that perpetrators of crimes Google the victims of crimes.

Initially, I observe that Trooper Follmer's belief that the perpetrator researched the victim and/or her address using Google was not expressly or inferentially tied to any of preceding beliefs he stated about the incident. It was tacked on to the end of his other hypotheses as an independent allegation not only untethered to the hunches that preceded it, but antithetical to the express hypothesis that the perpetrator knew the victim's address because he followed her back to her house. The Superior Court accepted those hunches as the predicate beliefs that give rise to the "reasonable probability" that the perpetrator searched for the victim and/or her address using Google. *Kurtz*, 294 A.3d at 523.[37] Likewise, the Commonwealth argues that the "incident and the crime were planned. This is illustrated by location of the residence, the drop off location, and the victim's schedule. The actor would have used the internet to facilitate the planning and commission of the crime." Commonwealth's Brief at 43. But common sense told Trooper Follmer that these factors led to the reasonable belief that the perpetrator had followed the victim home.

Nonetheless, many of those predicate beliefs in the affidavit are speculative hunches that do not individually or collectively establish probable cause to search Google's vast database of keyword searches. We must first delineate between the asserted facts and Trooper Follmer's hunches. The actual factual averments were not disputed by Kurtz, including the victim's account of how the crime transpired, the remote

[37] The Superior Court further relied on Trooper Follmer's testimony at the suppression hearing to make this link. *See Kurtz*, 294 A.3d at 523. Rule 203(D) expressly prohibits judicial review of probable cause using evidence other than what is found inside the four corners of the affidavit of probable cause. *See* Pa.R.Crim.P. 203(D).

location of her home, and that her husband was not present at the time of the offense due to his work schedule. Those facts provide no justification for a search of Google's databases. Trooper Follmer made no averments regarding witnesses or physical evidence tending to suggest that the perpetrator used any of Google's services to plan, execute, or cover-up the crimes committed.

The first hunch presented in the affidavit of probable cause was that the perpetrator was "very familiar" with the victim and not "randomly targeted" based "off the assessment of the incident." Affidavit of Probable Cause, 9/14/2016, at 1. Neither of these facts provides any obvious nexus to Google, even if they support the proposition that the victim was not randomly targeted. As Kurtz explains, these "speculative beliefs ... do not establish probable cause, because there was no evidence of articulable facts, reliable information, or reasonable inquiries that related to the use of Google by the perpetrator of the crimes" to identify or locate the victim or her home. Kurtz's Brief at 36-37. I agree with Kurtz.

The remoteness of the victim's home suggests that it was unlikely that the perpetrator simply stumbled upon the location at random. That proposition is fair enough. So how did the perpetrator find it? Is it reasonably probable that the perpetrator used Google simply because the home was remote? We know the victim's address was one of the key phrases that was targeted by the warrant application. That presupposes that the perpetrator already knew her address. If already familiar with the victim to the extent that the perpetrator knew her address and entered that information into a search bar, then he obviously did not require a search engine to discover the victim's address.

Furthermore, why did Trooper Follmer seek a warrant to search Google Maps for address searches rather than Apple Maps? Nothing within the four corners of the affidavit

of probable cause offers any explanation for his focus on Google Maps.[38] The perpetrator could have simply followed the victim to her home, conducted reconnaissance, and struck when it was clear that she was alone. Nothing in the affidavit of probable cause explains why Google was used under the limited facts of this case.

Moreover, the universe of individuals who were just as likely to have used Google Maps to navigate to or simply look up the victim's home in the week prior to the incident in question is potentially vast. The most obvious examples would be friends and family attempting to navigate to the victim's remote home. But the same inquiry is likely to be made by delivery drivers, utility workers, or any other person who has a reason to visit the victim's home without any intent to commit a crime. The near universal usage of Google or similar services in today's society is not a fact that narrows the focus of a search warrant to encompass those engaged in criminal conduct; the myriad of potential innocent uses of the technology for the same general purpose is precisely what makes it ubiquitous. The remoteness of the victim's home does not demonstrate anything above and beyond Trooper Follmer's bare hunch that the perpetrator might have used one of Google's search engines.

Next, Trooper Follmer stated his belief in the affidavit of probable cause that the perpetrator must have known that the victim's husband was not home when he attacked. Given the facts of this case, I agree that such a conclusion was reasonable. But that also does not tend to demonstrate in any way that the perpetrator utilized Google's search engine in committing his crime. As discussed, the affidavit presented an obvious theory

---

[38] While Google's keyword search engine may be ubiquitous, I am far less convinced the same label applies to its mapping service. Numerous apps are available for navigation purposes, perhaps most obvious being the one provided by Apple. No facts were provided in the affidavit of probable cause explaining why the perpetrator could not have used Apple Maps or any other available alternative. Trooper Follmer was operating based on a hunch that Google Maps had been used rather than providing a reasonable explanation supporting that assumption.

that would explain how the perpetrator could have known that the victim was alone—the perpetrator was stalking the victim before the attack occurred. The perpetrator could have developed an understanding of the husband's work schedule by spending time observing the comings and goings of the victim and her husband. *See* Affidavit of Probable Cause at 1 ("It is also believed that the Actor knew that the VICTIM'S husband was not at home at the time" and "may have spent some time stalking the VICTIM **and her husband's schedule** as well as **their whereabouts**.") (emphasis added). The perpetrator also could have observed the husband leaving on the night in question and determined that he was working a late shift (either by following the husband to his job or making a calculated guess). There are many possibilities as to how a plotting rapist might come to know or have a practical understanding of the husband's work schedule, but one theory makes no sense at all. It is patently unreasonable to assume the perpetrator ascertained the husband's work schedule by looking up the victim's name and address on Google. Nothing in the affidavit of probable cause tells us how the perpetrator's probable knowledge of the husband's work schedule was related to a Google search.

The fact that the victim was dropped off at a location that was near her home also provides no additional support for probable cause. Once the perpetrator knew the victim's address, no additional Google search was required to find a remote location near her remote home, particularly if the perpetrator had followed the victim home as Trooper Follmer specifically posited in the affidavit.

Kurtz is unquestionably correct that Trooper Follmer "did not have any evidence (such as a witness' statement, visual observations of the suspect by law enforcement, or a suspect's admission) to suggest that Google or any electronic device was used to commit the crimes in question." Kurtz's Brief at 36. Instead, Trooper Follmer simply had a hunch that the perpetrator might have used Google while plotting his crime. Nothing in

the affidavit of probable cause reasonably supports that hunch, even if we close our eyes to the fact that the affidavit of probable cause did not attempt to show a nexus between the undisputed facts, Trooper Follmer's hunches based on those facts, and Google's search database.[39]

What we have here is a modern version of a general warrant or a writ of assistance—a warrant lacking individualized suspicion and permitting law enforcement to engage in a fishing expedition. It is undisputed that there was no individualized suspicion targeting Kurtz; to the contrary, the purpose of the at-issue keyword search warrant was an attempt to discover the identity of an unknown assailant. That, by itself, is not fatal to the search warrant. However, there was also no individualized suspicion with respect to the location to be searched. By analogy, APP warrants are only permissible, as Justice Flaherty articulated in *Gilliam*, when "the affidavit in support of the warrant makes out a sufficient nexus between" the location to be searched "and the likelihood that every person present at that location is involved in the criminal activity at issue." *Gilliam*, 560 A.2d at 142-43 (Opinion in Support of Reversal).

Something akin to this location-based criterion for APP warrants is simply absent in this case. Clearly Google's vast database—the location to be searched—does not contain only information from individuals for whom law enforcement had probable cause to believe were engaged in unlawful activity, nor does it contain information from persons likely to be engaged in criminal activity. Indeed, even if we ignore the actual scope of the

---

[39] In her Concurring Opinion, Chief Justice Todd concludes that by "viewing the affidavit with a common sense, nontechnical, and ungrudging eye, and considering the totality of circumstances … that the affidavit demonstrates a 'fair probability' that Google searches were conducted in the planning or committing of the rape of K.M. and that Google search information would provide evidence of the crime, thereby supporting the issuance of a search warrant." Concurring Opinion at 11. But the Chief Justice conducts virtually no analysis of the affidavit of probable cause at all and simply accepts Trooper Follmer's hunches at face value. An "ungrudging eye" need not be an entirely blind one.

keyword search warrant (which effectively searched stored data from every Google user for a match), it cannot even be said that the universe of individuals identified by Google who merely searched for the victim's name and address would be limited to individuals for whom law enforcement had probable cause to suspect of involvement in the victim's kidnapping and rape. The ubiquity of Google as a search engine undermines any such suggestion. Applying the rationale developed in APP cases,[40] the warrant issued in this case must fail for lack of probable cause because there has been no nexus established between the location of the search (Google's database of stored user information) and the likelihood that data found there will only belong to persons for whom police are likely to have probable cause to believe committed a crime based on the facts articulated in the affidavit of probable cause.

Furthermore, this case does not involve "special needs" that go beyond the "normal need for law enforcement." *See Mistler*, 912 A.2d at 1271 (quoting *City of Indianapolis*, 531 U.S. at 37). Trooper Follmer was investigating a single criminal episode when he filed the warrant application.

Thus, I believe the warrant in this case was unlawful for want of individualized suspicion as is generally required for a finding of probable cause. *Jacoby*, 170 A.3d at 1084. The keyword search warrant was issued based on a bald hunch that evidence related to the victim's kidnapping and rape would be discovered, and the warrant it was fatally devoid of any individualized suspicion targeting Kurtz or the location to be searched. The Commonwealth concedes these two basic defects in the issuing authority's finding of probable cause, stating the "search warrant for Google, Inc. was supported by probable cause even though the suspect is unknown and there was no

[40] We note again that APP warrants have never been condoned by a Majority of this Court.

direct evidence that Google ... was used in the commission of the crime." Commonwealth's Brief at 39. The Commonwealth urges that we overlook these defects but provides no principled basis for doing so.[41]

If this Court ever concludes that APP warrants comport with Article I, Section 8, I believe a keyword search warrant might satisfy the APP warrant standard adopted by a majority of jurisdictions that have addressed it. This would require that police provide sufficiently unique terms or limitations that would meet the probable cause standard. For instance, probable cause might exist for a keyword search warrant for anyone who searched for a specific unique item used in the commission of an offense (e.g., an exotic poison that could only be administered under unique conditions) **and** searched for the victim's address or name in the days preceding the crime in which such items were used. A more direct nexus between a crime and the use of a search engine might also arise when a victim or witness directly observes a perpetrator's use of a search engine during the commission of a crime. Here, however, the only links between the facts provided in the affidavit of probable cause and Google's search engines were wholly conclusory assumptions about the ubiquity of search engines. Probable cause demands more.

---

[41] The one case arising in a foreign jurisdiction addressing a keyword search warrant, *Seymour*, does not provide any reason to sanction keyword search warrants generally or under the facts of this case. In that case, the police sought a search warrant "for a list of any users who had searched one of nine variations of" the targeted address in a two-week period before an arson that resulted in death. *Seymour*, 536 P.3d at 1268. After ruling out several of the IP addresses discovered by the search, the police identified Seymour and charged him with arson and murder. Seymour challenged the warrant on probable cause grounds, arguing that it lacked individualized suspicion. However, the Colorado Supreme Court did not decide the question, holding that Colorado's good-faith exception to its exclusionary rule applied even if probable cause was lacking. *Id*. at 1278. Nonetheless, the *Seymour* Court observed that the probable cause question was "at least debatable" despite the broad deference afforded to the issuing authority's determination of probable cause, observing that "people search addresses for much more innocuous reasons all the time" and "if the perpetrators were targeting the victims, one might assume that they were sufficiently familiar with them to dispense with searching the address." *Id*.

For the reasons set forth above, I would conclude that Trooper Follmer's affidavit failed to establish probable cause to conduct a keyword search of Google's database under the facts of this case. No evidence nor reasonable assumptions derived therefrom provide a clear nexus between the criminal activity under investigation and the location to be searched. However, I remain open in future cases to the possibility that probable cause could be established to obtain a keyword search warrant under a different fact pattern where there is evidence that clearly suggests a perpetrator utilized a search engine to facilitate criminal activity. The circumstances of this case do not approach such a showing.

IV. Conclusion

In response to the questions this Court accepted for review, I would hold that citizens possess a reasonable expectation of privacy in their internet search queries under Article I, Section 8 of the Pennsylvania Constitution. Furthermore, because probable cause was lacking to show a nexus between the criminal activity under investigation and the location to be searched, I would reverse the order denying suppression.

I respectfully dissent.