Received 1/5/2024 10:37:58 AM Supreme Court Middle District

Filed 1/5/2024 10:37:00 AM Supreme Court Middle District
98-100 MAP 2023

IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

No. 98-100 MAP 2023

COMMONWEALTH OF PENNSYLVANIA,

Appellee,

v.

JOHN EDWARD KURTZ,

Appellant.

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND PENNSYLVANIA ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF APPELLANT AND REVERSAL

On Appeal from the Order of the Superior Court at Nos. 811, 421 & 429 MDA 2023 entered on April 28, 2023, Affirming the Judgment of Sentence of the Northumberland County Court of Common Pleas, Criminal Division, at No. CP-49-CR-0001479-2018 entered on March 2, 2021

Jeremy D. Mishkin (PA No. 30017)
Montgomery McCracken Walker & Rhoads LLP
1735 Market Street
Philadelphia, PA 19103-7505
(215) 772-7246
jmishkin@mmwr.com

On the brief:

Andrew Crocker
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation

Daniella Gordon (PA No. 201477)
Third Circuit Vice Chair
NACDL Amicus Committee
McCarter & English, LLP
1600 Market Street, Suite 3900
Philadelphia, PA 19103
(215) 979-3812
dgordon@McCarter.com

Michael Price
Fourth Amendment Center
NACDL
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 465-7615
mprice@nacdl.org

Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers

Patrick A. Casey (PA No. 50626)
PACDL President
Myers, Brier & Kelly, LLP
425 Biden Street, Suite 200
Scranton, PA 18503
(570) 342-6100
pcasey@mbklaw.com

Attorney for Amicus Curiae Pennsylvania Association of Criminal Defense Lawyers

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization. Founded in 1990, EFF has over 35,000 active donors and dues-paying members across the United States, including in Pennsylvania. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as amicus in the U.S. Supreme Court, this Court, and many others in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g., Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *Commonwealth v. Pacheco*, 263 A.3d 626 (Pa. 2021); *People v. Seymour*, 536 P.3d 1260 (Colo. 2023).

The National Association of Criminal Defense Lawyers ("NACDL") is a non-profit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers, with tens of thousands of members and affiliates throughout the country. NACDL is particularly interested in

[1] Amici certify, pursuant to Rule 531(b)(2) of the Pennsylvania Rules of Appellate Procedure, that no person or entity, other than Amici, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

cases arising from surveillance technologies and programs that pose new challenges to personal privacy. It operates a dedicated initiative that trains and directly assists defense lawyers handling such cases to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in this Court and the Supreme Court on digital privacy and criminal justice issues, including: *League of Women Voters of Pennsylvania v. DeGraffenreid*, 265 A.3d 207 (Pa. 2021); *Kuren v. Luzerne Cnty*., 146 A.3d 715 (Pa. 2016); *Carpenter*, 138 S. Ct. at 2211; *Riley*, 573 U.S. at 377; *United States v. Jones*, 565 U.S. 400 (2012).

The Pennsylvania Association of Criminal Defense Lawyers ("PACDL") is a professional association of attorneys admitted to practice in Pennsylvania and actively engaged in criminal defense representation. Founded in 1988, PACDL is the Pennsylvania affiliate of the National Association of Criminal Defense Lawyers. As Amicus Curiae, PACDL represents the experience and perspective of Pennsylvania's professional criminal defense lawyers including private practitioners, public defenders, and academics who seek to protect and ensure by rule of law those individual rights guaranteed by the Pennsylvania and United States Constitutions, and who work to achieve justice and dignity for defendants and thus for all citizens and residents of the Commonwealth. PACDL membership currently includes more than 850 private criminal defense practitioners and public defenders throughout the Commonwealth. PACDL regularly files amicus curiae

briefs in this Court in matters of particular importance to Pennsylvania criminal law.

INTRODUCTION

The Internet is crucial to our understanding of and engagement with the world, but it can be nearly impossible to navigate the billions of websites without the use of a search engine like Google. Users have come to rely on search engines to such a degree that they routinely search for the answers to sensitive or unflattering questions that they might never feel comfortable asking a human confidant. Yet as is clear from this case, Google retains detailed information on the search queries of everyone who uses its search engine. Over the course of months and years, there is little about users' lives that will not be reflected in their search keywords, from the mundane to the most intimate. The result is a vast record of some of users' most private and personal thoughts, opinions, and associations.

Because of the breadth and detailed nature of search query data, keyword search warrants like the one in this case are especially concerning. Keyword search warrants are unlike typical warrants for electronic information in a crucial way: they are not targeted to specific individuals or accounts. Instead, they require a provider to search its entire reserve of user data and identify any and all users or devices who searched for words or phrases specified by police. As in this case, the police generally have no identified suspects when they seek a keyword search

warrant. Instead, the sole basis for the warrant is the officer's hunch that the perpetrator might have searched for something related to the crime.

Hence, keyword warrants are dragnet searches. Like 18th-century writs of assistance that inspired the drafters of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution, keyword warrants are general warrants that permit police to conduct "a general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). They are therefore prohibited by both the Fourth Amendment and the Pennsylvania Constitution. *Id.*; *Commonwealth v. Edmunds*, 586 A.2d 887, 897 (Pa. 1991). And like those writs, keyword warrants are especially pernicious because they target protected speech and the corollary right to receive information. *See Stanford v. Texas*, 379 U.S. 476, 482–83 (1965); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1051–52 (Colo. 2002) (en banc), *as modified on denial of reh'g* (Apr. 29, 2002). For this reason, they must be examined with heightened scrutiny. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 565 (1978). The same concerns animating the courts that addressed general warrants in the past are equally present with respect to keyword warrants today; these warrants lack individualized suspicion, allow for unbridled officer discretion, and impact the privacy rights of countless innocent individuals. Because the warrant in this case targets speech, lacks probable cause, and is

overbroad, it violates both the Pennsylvania and federal constitutions and should have been suppressed.

ARGUMENT

I. Keyword Warrants Draw on Vast Repositories of Data Held by Search Engines, Authorizing Indiscriminate Interference with Internet Users' Privacy.

A. Search Engines Are Indispensable to Browsing the Internet.

Keyword warrants are enabled because it is virtually impossible to find a website or any other information on the Internet without entering search terms (also known as "keywords") into a search engine.

According to some sources, there are about 1.1 billion websites, and tens of billions of webpages.[2] Somewhat like how houses and businesses have street addresses in the physical world, each of those tens of billions of webpages has its own unique form of an address—called a URL ("uniform resource locator")—in the online world. The URL serves as both a location and as directions for a user's browser to load a particular webpage. URLs contain the website's domain name, which may be easy to remember or guess, like "Google.com," but they contain additional information after the domain name, which may be much more complex.

[2] *November 2023 Web Server Survey*, Netcraft (Nov 24, 2023), https://www.netcraft.com/blog/november-2023-web-server-survey/; *The size of the World Wide Web (The Internet)*, Tilburg University, https://www.worldwidewebsize.com/.

For example, the domain for the Pennsylvania courts website is pacourts.us, and the specific URL for instructions for where to file a brief in the Pennsylvania Supreme Court is https://www.pacourts.us/courts/supreme-court/prothonotarys-addresses. URLs may be quite long and are often "dynamic," meaning they change based on users' search queries, among other circumstances.[3] For example, to get directions to this Court using Google Maps, one would need to enter: https://www.google.com/maps/place/601+Commonwealth+Ave,+Harrisburg,+PA+17120/@40.2670348,-76.8847218,17z/—or just use a search engine.

Search engines make it possible to find not just websites, but also specific content within websites, including text, video, images, and documents. Search engines continuously scour the Internet for content, index and organize the information they find into vast databases, and rank that information based on its relevance to search queries.[4]

The keywords that users type into search engines can be incredibly revealing. Internet users frequently search for specific addresses, answers to medical questions, information about controversial ideas, and discussions of

---

[3] Vangie Beal, *Dynamic URL*, Webopedia (May 24, 2021), https://www.webopedia.com/TERM/D/dynamic_URL.html.

[4] *Web crawler*, Wikipedia, https://en.wikipedia.org/wiki/Web_crawler; *How Google Search Works*, Google, https://www.google.com/search/howsearchworks/how-search-works.

gender and sexuality, to give just a few examples out of the nearly limitless possibilities. Specialized users may search for seemingly more "incriminating" information. A crime novelist could search for unique ways to kill people, a historian of the civil rights era could search for racist language, or a policy analyst could search for specifics on how drugs are manufactured and used. Some of the top questions posed to Google are "War in Israel and Gaza," "how to get pregnant," and "how to have sex."[5] Even a simple query for an address can be revealing. For example, knowing that a person searched for "1514 N 2nd St, Harrisburg," could lead to an inference that the person was seeking an abortion. (This is the address of Planned Parenthood.) Searches can be so specific to an individual that even the most innocuous queries can quickly reveal their identity. In 2006, AOL published three months of de-identified search history data from 650,000 users.[6] With that data, the *New York Times* was easily able to identify

[5] *Year in Search 2023*, Google, https://trends.google.com/trends/yis/2023/US/; *The Most Asked Questions on Google*, Mondovo, https://www.mondovo.com/keywords/most-asked-questions-on-google.

[6] Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TechCrunch (Aug. 6, 2006), https://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data.

"Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs."[7]

Under some circumstances, users' search queries may differ from those they intended. Modern search engines offer an "autocomplete" feature, which relies on sophisticated algorithms to make predictions about what the user might be looking for based on data like the user's geographic location, their past search queries, their language, and "common and trending queries."[8] Search engines provide a list of five to ten contextualized suggestions almost immediately after the user starts typing a query, and those suggestions change as a user types in more letters.[9] This feature can be particularly helpful when searching on a mobile device's smaller screen and letter keys. However, it can also lead to users entering unintended queries, which may be particularly true with less-common queries, such as addresses.

---

[7] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. Times (Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol.html.

[8] Danny Sullivan, *How Google autocomplete predictions are generated*, Google (Oct. 8, 2020), https://blog.google/products/search/how-google-autocomplete-predictions-work.

[9] Danny Sullivan, *How Google autocomplete works in search*, Google (Apr. 20, 2018), https://www.blog.google/products/search/how-google-autocomplete-works-search.

Google Search is far and away the most popular search engine, with nearly 92% worldwide market share (89% in the United States),[10] and "more than 1 billion average monthly users."[11] Most people use Google to search the Internet at least three times per day,[12] and Google reportedly processes nearly 100,000 search queries every second.[13] This translates to over 8.5 billion searches per day.[14] As of 2019, 63% of those searches were conducted on mobile devices.[15]

Due to its market dominance, Google possesses massive amounts of information about users' searches. For users logged into their accounts, Google keeps a record of all search queries and stores that data along with other information about the user, including what videos they have watched, what images they have viewed, what websites they have visited, where they have traveled, and

---

[10] *Search Engine Market Share in 2023*, Oberlo, https://www.oberlo.com/statistics/search-engine-market-share.

[11] *See Seymour*, 536 P.3d at 1268 (Seymour C.A.R. 21 Petition, Exh. 4, Decl. of Nikki Adeli ¶ 4), *available at* https://www.eff.org/document/people-v-seymour-google-declaration-colorado-keyword-search (hereinafter "Google Decl."); *see also* R. at 275:13-14 (Testimony of Trooper Joel Follmer stating the police believed a warrant to Google would yield evidence because "Google . . . is the number one search engine in the world")

[12] Maryam Mohsin, *10 Google Search Statistics You Need to Know in 2023*, Oberlo (Jan. 13, 2023), https://www.oberlo.com/blog/google-search-statistics.

[13] *Id*.

[14] *Id*.

[15] *Id.*

who they are.[16] Google now allows users to delete search history and to turn off Google's collection of that data.[17] However, if users do not take active steps to delete their data, Google will likely have a record of everything they have ever searched for, dating back years.[18]

Even turning off Google's data collection does not stop Google from tracking queries; it only divorces that collection from other details in a user's account. Google retains data on *anyone* who uses its search engine, not just Google users who are logged into their accounts. Google links each search to a device's IP address and, using that information, an officer can easily connect that search to a specific person.[19] Given this, it is very difficult to search Google anonymously. This is true whether users are searching using a personal computer or a handheld device.[20] It is unclear how long Google retains search history data from people who

---

[16] *See Access & control activity in your account*, Google, https://support.google.com/accounts/answer/7028918.

[17] *Id.*

[18] Luke Johnson, *How to see EVERY Google search you've ever made*, Digital Spy (Dec. 26, 2016), https://www.digitalspy.com/tech/a805172/how-to-see-every-google-search-youve-ever-made.

[19] *See, e.g.,* R. at 177a–78a (data provided by Google in its response to the search warrant at issue in this case); R. at 277a–78a (testimony of Trooper Joel Follmer describing process used to identify a person of interest).

[20] For Android device users, it is particularly difficult to search without being logged into a Google account. David Nield, *A Guide to Using Android Without Selling Your Soul to Google*, Gizmodo (July 26, 2018), https://gizmodo.com/a-guide-to-using-android-without-selling-your-soul-to-g-1827875582.

are not logged into Google accounts, but if it is anything like other data Google collects on users, Google's database could go back a decade or more.[21]

B. Keyword Warrants Allow Access to Billions of Users' Search Queries and Have the Potential to Implicate Innocent People.

The use of keyword search warrants is relatively new—the 2016 warrant in this case predates even their first reports in the press[22]—and it is unclear how many are issued each year. Google produces public reports that include the total number of warrants it receives every six months, but it does not break out the number of keyword warrants.[23] If keyword warrants are anything like another novel dragnet method used to identify suspects—"geofence warrants"[24]—their use is likely increasing year over year. Geofence warrants now make up 25% of all warrants

---

[21] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (noting at the time of publication, Google's Location History data goes back nearly a decade).

[22] Thomas Brewster, *Cops Demand Google Data on Anyone Who Searched a Person's Name... Across a Whole City*, Forbes (Mar. 17, 2017), https://www.forbes.com/sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/?sh=5fe5045d7ade.

[23] *See Global requests for user information—United States*, Google, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period.

[24] Geofence warrants seek information on every device that might have been within designated geographic areas and time periods in the past.

Google receives, and in Pennsylvania, the number of geofence warrants increased by a factor of more than 30 between 2018 and 2020.[25]

Several known keyword warrants have, as in this case, sought to identify everyone who searched for a specific address or variations of the victim's name.[26] However, in other cases police have investigated other search queries, such as the name of someone else related to the case.[27] In at least two known cases, the search queries have been far broader. In response to a series of bombings in Austin, Texas, police sought everyone who searched for words like "low explosives" and "pipe bomb."[28] And in Brazil, Google challenged a warrant for everyone who

---

[25] *Supplemental Information on Geofence Warrants in the United States*, Google, at 2 (2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (follow "Download supplemental data as a CSV" hyperlink).

[26] *See, e.g.*, Siladitya Ray, *Google Shared Search Data With Feds Investigating R. Kelly Victim Intimidation Case*, Forbes (Oct. 8, 2020), https://www.forbes.com/sites/siladityaray/2020/10/08/google-shared-search-data-with-feds-investigating-r-kelly-victim-intimidation-case/?sh=7a4a7b847c62.

[27] Brewster, *Cops Demand Google Data On Anyone Who Searched A Person's Name... Across A Whole City*, *supra* n.22; Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched A Sexual Assault Victim's Name, Address or Telephone Number*, Forbes (Oct. 4, 2021), https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=545cc7b87c97.

[28] Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address or Telephone Number*, *supra* n.27.

searched for the name of a popular politician who was assassinated and the busy street in Rio de Janeiro where she was killed.[29]

Google has stated it must search its entire database of users' search queries within the relevant time period to comply with a keyword warrant, including users well outside the area of the crime.[30] This is because the warrant does not identify a particular account or device but instead seeks *any* device that may have searched for the specified terms during the relevant time period. Although Google may not immediately turn over full identifying information about users who searched for specific keywords in response to a keyword warrant,[31] at least in this case Google provided enough information in the first step—full IP addresses—to allow the police to identify the source for each of the search queries.[32] If police know the ISP or carrier in addition to the IP address,[33] they do not need Google to determine the source of the search query; instead, in most cases, they can submit a simple

---

[29] Naomi Gilens, et al., *Google Fights Dragnet Warrant for Users' Search Histories Overseas While Continuing to Give Data to Police in the U.S.*, EFF (Apr. 5, 2022), https://www.eff.org/deeplinks/2022/04/google-fights-dragnet-warrant-users-search-histories-overseas-while-continuing.

[30] *See* Google Decl. ¶ 4.

[31] Google Decl. ¶¶ 7–9 (describing process).

[32] See R. at 277a–78a (testimony of Trooper Joel Follmer describing process used to identify a person of interest).

[33] It is possible to determine the ISP associated with an IP address using a simple lookup tool, such as https://www.whatismyip.com/ip-address-lookup.

subpoena to the carrier for billing records—including name and address—associated with that IP address.[34]

Because keyword warrants require Google to search its entire data repository, they have the potential to implicate innocent people who happen to search for something an officer believes is incriminating. Here, Google identified responsive queries from fourteen different IP addresses within the eight days covered by the warrant.[35] Keyword warrants could also allow officers to target people based on political speech and by their association with others. Police used multiple geofence warrants to identify people at political protests in Kenosha, Wisconsin, and Minneapolis after police killings in those cities.[36] Similarly, with keyword warrants, officers could seek to identify everyone who searched for the location or the organizers of a protest.

---

[34] *See* 18 U.S.C. § 2703(c)(2).

[35] R. at 277a:2–3 (testimony of John Follmer).

[36] Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson*, Forbes (Aug. 31, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-dragnets-on-phone-data-across-13-kenosha-protest-arsons; Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TechCrunch (Feb. 6, 2021), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant.

II. Keyword Warrants Harm Expressive Freedoms and Are Subject to Heightened Fourth Amendment Scrutiny.

A. Keyword Warrants Compromise Expressive Freedoms.

Keyword warrants do not just authorize indiscriminate interference with privacy rights, they also compromise protections for expressive freedoms guaranteed by the First Amendment and Article I, Section 7 of the Pennsylvania Constitution.

By targeting Google users' search queries, the keyword warrant is directed entirely at expressive activity, beginning with the literal words of the targeted queries. But because search engines are an indispensable tool for finding information on the Internet, querying a search engine implicates not just constitutional free speech rights, but also the rights to distribute and receive information, and to freely and privately associate with others.

The U.S. Supreme Court has held repeatedly that the right to receive information is a "corollary of the rights of free speech and press" belonging to both speakers and their audience. *Board of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (plurality op.); *see also Kleindienst v. Mandel*, 408 U.S. 753, 762–763 (1972) (cataloging right to receive information in a "variety of contexts"); *Martin v. City of Struthers*, 319 U.S. 141, 146-47 (1943). A speaker's exercise of the freedom to speak and disseminate information would be futile if others were prohibited from receiving it. "It would be a barren marketplace of ideas that had only sellers and no

buyers." *Pico*, 457 U.S. at 867 (quoting *Lamont v. Postmaster Gen.*, 381 U.S. 301, 308 (1965) (Brennan, J., concurring)).

The right to receive information is also "a necessary predicate to the recipient's meaningful exercise of his *own* rights of speech, press, and political freedom." *Pico*, 457 U.S. at 867 (emphasis added). It is through listening to others' speech that "our personalities are formed and expressed" and "our convictions and beliefs are influenced, expressed, and tested" so that we can "bring those beliefs to bear on Government and on society." *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 817 (2000). Hence, "[t]he citizen is entitled to seek out or reject certain ideas or influences without Government interference or control." *Id.*; *Stanley v. Georgia*, 394 U.S. 557, 565 (1969).

As a result, the U.S. Supreme Court and other courts have expressed special concern for government attempts to discover people's interest in specific reading material. *See id.*; *Tattered Cover*, 44 P.3d at 1051 (requiring heightened showing and adversarial hearing before enforcing warrant to bookstore for customer purchase records); *In re Grand Jury Subpoena to Kramerbooks & Afterwords*, 26 Med. L. Rptr. 1599, 1601 (D.D.C. 1998) (heightened showing required for subpoena for individual customer's book purchases); *In re Grand Jury Subpoena to Amazon.com Dated August 7, 2006*, 246 F.R.D. 570, 571-73 (W.D. Wis. 2007) (quashing subpoena for identities of 120 book buyers) ("[I]t is an unsettling and

un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while hunting for evidence against somebody else."). Searches of places such as bookstores and libraries that allow people to look for and access reading material are especially disfavored. "Once the government can demand of a publisher the names of the purchasers of his publications, ... [f]ear of criticism goes with every person into the bookstall." *United States v. Rumely*, 345 U.S. 41, 57 (1953) (Douglas, J., concurring). As the Colorado Supreme Court held in *Tattered Cover*, readers are entitled to anonymity in requesting information "because of the chilling effects that can result from disclosure of identity." 44 P.3d at 1052 (citing *McIntyre v. Ohio*, 514 U.S. 334, 357 (1995); *Talley v. California*, 362 U.S. 60, 64–65 (1960)).

Investigations of users' online search queries raise identical concerns to investigations seeking records held by physical bookstores and libraries. Like bookstores, search engines are "places where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable." *Tattered Cover*, 44 P.3d at 1052. And as with reading lists, disclosure of users' search queries chills their right to seek out information and deters participation in the "uninhibited, robust, and wide-open debate and discussion" contemplated by the Constitution. *Lamont*, 381 U.S. at 307; *see also Tattered Cover*, 44 P.3d at

1050 (detailing evidence that search warrant for bookstore's patron list deterred customers' willingness to purchase "controversial books").

B. Given the Expressive Freedoms Implicated by the Keyword Warrant, the Fourth Amendment Must Be Applied with "Scrupulous Exactitude."

When a government search directly implicates expressive activity, the U.S. Supreme Court has required that the Fourth Amendment "preconditions for a warrant—probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness" be applied with "scrupulous exactitude." *Zurcher*, 436 U.S. at 565, 564 (quoting *Stanford*, 379 U.S. at 485); *see also Commonwealth v. Santner*, 454 A.2d 24, 31 (Pa. Super. Ct. 1982) (citing *Stanford* and suppressing warrant that resulted in seizure of medical records reflecting what "patients had told their doctor"). In this case, these preconditions were not met with anything approaching scrupulous exactitude. Instead, the keyword warrant was an unconstitutional general warrant.

III. The Keyword Warrant Was an Unconstitutional General Warrant in Violation of the Fourth Amendment and Article I, Section 8.

A. Under Both the Federal and Pennsylvania Constitutions, Individuals Maintain an Expectation of Privacy in Their Search Queries and Associated Data.

Contrary to the holding of the court below, precedent from the U.S. Supreme Court and this Court establishes that Internet users maintain an expectation of privacy in their search queries and associated records. *See Commonwealth v. Kurtz*,

294 A.3d 509, 520 (Pa. Super. Ct. 2023). Search queries are among the most sensitive digital communications, which are protected as the modern equivalent of "papers and effects" enshrined in the Fourth Amendment. *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) ("The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities."). Like the location data in *Carpenter* that the U.S. Supreme Court held is protected by the Fourth Amendment, "an individual's Google search history 'hold[s] for many Americans the privacies of life.'" *Seymour*, 536 P.3d at 1271 (quoting *Carpenter*, 138 S. Ct. at 2217)[37]; *Riley*, 573 U.S. at 395 ("An Internet search and browsing history. . . could reveal an individual's private interests or concerns.")

Because of the sensitive and private information contained in our digital communications, courts have recognized they are entitled to constitutional protections even though they are transmitted by and stored with third parties like Google. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010)

[37] In *Seymour*, the Colorado Supreme Court assumed without deciding that a keyword warrant lacked probable cause as to the users searched but upheld the warrant on the good faith exception. *Seymour*, 536 P.3d at 1268. However, "the good-faith exception does not exist under Pennsylvania law." *Commonwealth v. Carper*, 172 A.3d 613, 618 (Pa. Super. Ct. 2017) (cleaned up).

(Fourth Amendment protects email stored by ISP).[38] Search queries are highly analogous to these other communications. *See, e.g., In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 138–39 (3rd Cir. 2015) (search queries as "content" of communications). Courts have also identified certain business records—like the customer book purchase records discussed above—that are maintained by third parties but are nevertheless constitutionally protected due to their potentially sensitive nature and the chilling effects that could result from their disclosure. *See e.g., Carpenter*, 138 S. Ct. at 2217; *Tattered Cover*, 44 P.3d at 1051. Search queries and the responsive records at issue in this case are no different. The information sought by the warrant in this case did not merely reveal a specific individual's IP address; it connected that IP address to a specific query and also identified the IP addresses of *anyone* had searched for specific phrases. And Google's production included IP addresses for individuals who searched for words and terms not named in the warrant itself. *Compare* R. at 172a (warrant attachment requesting identities of users who searched for victim's

[38] Since *Warshak*, courts have routinely held that individuals have a reasonable expectation of privacy in their email held in accounts operated by third party providers. The U.S. Supreme Court has agreed, at least in dicta; in the Court's opinion in *Carpenter*, every Justice authored or joined an opinion acknowledging that the Fourth Amendment protects the content of stored digital files. *See* 138 S. Ct. at 2222 (majority op., Roberts, C. J., joined by Ginsburg, Breyer, Sotomayor, and Kagan, JJ.); *id.* at 2230 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); *id.* at 2262, 2269 (Gorsuch, J., dissenting).

name and address) *with* R. at 177a. (Google production, which also included users who searched for victim's address and "woman abducted"). In other words, the government learned not just the IP addresses themselves, but also the contents of communications linked to these IP addresses. *In re Google Inc. Cookie Placement,* 806 F.3d at 138.

Moreover, this Court has applied the "third party doctrine" under Article I, Section 8 of the Pennsylvania Constitution in a narrower set of circumstances than the U.S. Supreme has under the Fourth Amendment. For example, under *United States v. Miller,* 425 U.S. 435 (1979), individuals lack a Fourth Amendment expectation of privacy in bank records because they are held by a third party. But under Article I, Section 8, the contents of bank records are *protected* because they reveal the depositor's "personal affairs, opinions, habits or associations." *Commonwealth v. Duncan,* 817 A.2d 455, 461, 463 (Pa. 2003) (quoting *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979)).[39] As described above, search queries can reveal the sort of "virtual current biography" that this Court held is protected in *DeJohn*. *Id.*

[39] In *Duncan*, this Court clarified that its holding in *DeJohn* rejecting application of the third party doctrine to "substantive" bank records was "different in kind" from the "disclosure of a mere name and address corresponding to a particular ATM card number." 817 A.2d at 463.

Finally, Google's terms of service (TOS) do not undercut users' expectation of privacy in their search queries. Like the email provider in *Warshak*, *see* 631 F.3d at 286, Google and every other major commercial service provider inform their users that the service reserves the right to access user information and disclose information to law enforcement to protect the business's interests, rights, and property. Nevertheless, in *Warshak* the Sixth Circuit concluded that this reservation of rights did not defeat an individual's reasonable expectation of privacy in email. *Id*.

The U.S. Supreme Court has also rejected the argument that private form contracts can limit or nullify a person's Fourth Amendment rights vis-à-vis the government. *See Byrd v. United States*, 138 S. Ct. 1518 (2018). In *Byrd*, the Court held that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement. *Id.* at 1529. Like terms of service, these agreements "concern risk allocation between private parties. . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car." *Id*.[40]

[40] Numerous other cases support the conclusion that private contracts do not undermine individuals' expectations of privacy. *See, e.g., Rakas v. Illinois*, 439 U.S. 128, 142, 143 (1978) ("arcane distinctions developed in property and tort law . . . ought not to control" the analysis of who has a "legally sufficient interest in a

Because all service providers impose TOS similar to Google's, the lower court's analysis, if correct, would apply to digital data maintained with any service provider, not just Google. Further, because providers' terms apply to *all* content they store, not just search queries, this analysis would apply to any and all emails, files, photos, attachments, and other electronic "papers and effects" stored with any of those providers. Not only would that conclusion vitiate Fourth Amendment protections for the hundreds of millions of people who use these services, it would mean that a private company's TOS trump Fourth Amendment protections for *all* content maintained with the provider. This is inconsistent with public expectations, well-recognized Fourth Amendment case law, and the stated positions of every member of the Supreme Court in *Carpenter*. If adopted by this Court, it would undermine fundamental privacy protections in communications media used by nearly all Americans.

B. The Fourth Amendment and Article I, Section 8 Were Drafted to Preclude General Warrants.

Cases like this one that involve the intersection of expressive freedoms and indiscriminate government searches directly motivated the drafting and adoption of

---

place"); *Smith v. Maryland*, 442 U.S. 735, 745 (1979) ("We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.").

the Fourth Amendment and the even more expansive protections in Article I, Section 8 of the Pennsylvania Constitution.

In the American colonies, British agents used general warrants, also known as "writs of assistance," to conduct broad searches for smuggled goods, limited only by the agents' own discretion. *See Stanford*, 379 U.S. at 481-82.[41] "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley*, 573 U.S. at 403.

General warrants had particularly pernicious effects on the exercise of expression freedoms. Discussing the British "use of general warrants as instruments of oppression," the U.S. Supreme Court commented that "this history is largely a history of conflict between the Crown and the press." *Stanford*, 379 U.S. at 482. In particular, two British cases of the 1760s, *Wilkes v. Wood* and *Entick v. Carrington*, both centered on general warrants intended to suppress allegedly libelous publications. *Id.* at 483. "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure

[41] *See also* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning,* 363, 602–1791 (2009).

could also be an instrument for stifling liberty of expression." *Id.* at 484; *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting) ("decisions granting recovery to parties arrested or searched under general warrants on suspicion of seditious libel" were "fresh in the colonists' minds"); *see also Commonwealth v. Grossman*, 555 A.2d 896, 899 & n.5 (Pa. 1989) (suppressing fruits of warrant that authorized seizure of broad categories of documents and noting similarity to general warrant at issue in *Entick*).

The primary purpose of both the Fourth Amendment and Article I Section 8, therefore, was to prohibit general warrants, especially those that authorized exploratory rummaging into individuals' protected expression. *Stanford*, 379 U.S. at 481 (Fourth Amendment "reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant"); *Commonwealth v. Waltson*, 724 A.2d 289, 291 (Pa. 1998) ("[T]he purpose underlying Article 1, Section 8 was to protect persons from unreasonable searches and seizures conducted pursuant to general warrants."). And this Court has noted that the Pennsylvania Constitution's protection against general warrants has an even more direct connection to the experience of the colonists. *Commonwealth v. Edmunds*, 586 A.2d 887, 896 (Pa. 1991) ("Pennsylvania's Constitution was drafted in the midst of the American

Revolution . . . . The Declaration of Rights in the Pennsylvania Constitution was an organic part of the state's original constitution of 1776, and appeared (not coincidentally) first in that document.").

C. Keyword Warrants Have Direct Parallels to General Warrants and Are Similarly Per Se Unconstitutional.

A warrant purporting to authorize a reverse keyword search is a digital analog to a warrant that authorizes officers to search every house in an area of a town—simply on the chance that they might find written material connected to a crime. Like the general warrants and writs of assistance used in England and colonial America, this warrant's lack of particularity and overbreadth invites the police to treat it as an excuse to conduct an unconstitutional general search. *See Commonwealth v. Johnson*, 240 A.3d 575, 584 (Pa. 2020) (citing *Commonwealth v. Matthews*, 285 A.2d 510, 514 (Pa. 1971)).

Here, the keyword "warrant specified only an offense" and left to law enforcement discretion "the decision as to which persons" should be pursued. *Steagald*, 451 U.S. at 220. The warrant did not name particular suspects or even particular accounts. Instead, based on no more than the state trooper's hunch, it sought information on *all* accounts associated with devices that might have searched for phrases potentially linked to the crime. But, with a proper search warrant, "nothing is left to the discretion of the officer executing the warrant." *Grossman*, 555 A.2d at 899 (quoting *Marron v. United States*, 275 U.S. 192, 196

(1927)). The keyword warrant is precisely the sort of "general, exploratory rummaging" the Fourth Amendment was intended to forestall. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *Andresen*, 427 U.S. at 479-480.

Both the Fourth Amendment and Article I, Section 8 require that warrants describe places to be searched and things to be seized with particularity, and the language of the Pennsylvania Constitution is even "more stringent." *Grossman*, 555 A.2d at 899. When a warrant's language is unduly broad or ambiguous, it is more likely to reach information for which there is no probable cause. *Id.* Where, as here, the categories of records sought are so sweeping as to include anyone who searched for a phrase, there is an "unreasonable discrepancy between the items for which there was probable cause and the description in the warrant" and thus "requires suppression." *Id*. at 900.

The warrant here is arguably broader than general warrants of the colonial period. *Id*. at 899. Keywords warrants require Google to search through *all* of its users' search data—*tens of millions* of user accounts—just to extract the subset of information responsive to the warrant.[42] And a warrant like this was not conceivable, much less possible, at the nation's founding. Retrospective search query data held by Google "gives police access to a category of information otherwise unknowable." *Carpenter*, 138 S. Ct. at 2218. Like cell site location

[42] Google Decl. ¶4.

information, it allows the police to "travel back in time" to reconstruct a person's queries. *Id*.

Search warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet" of information "to be seized at the discretion of the State." *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003). Searches like these—where the only information the police have is that a crime has occurred—are just that: a "dragnet" that implicates any and all innocent people who happen to have searched for information related to the specified keywords. *See* Section I.C, *supra*. Keyword warrants authorize Google to release data to the police that includes search history for people with no connection to the crime under investigation.[43] This kind of search turns every user into a suspect.

D. The Keyword Warrant in This Case Was Insufficiently Particularized and Lacked Probable Cause to Support a Search of Every Device.

Even if keyword warrants are not categorically unconstitutional general warrants, they must satisfy the requirements of particularity and probable cause on a case-by-case basis. *See Pacheco*, 263 A.3d at 646 (citing *Dalia v. United States*, 441 U.S. 238, 255 (1979)). The keyword warrant in this case failed to do so.

[43] In this case, Google disclosed fourteen unique IP addresses, which led police to two individuals who were not involved in the crime. R. at 277a–78a.

First, the warrant in this case was based on nothing more than an officer's speculation that the perpetrator may have used a search engine sometime within the eight days prior to the crime to look for the victim's house. The only stated connection to Google for this hunch was that its search engine is dominant, suggesting that if the perpetrator had conducted such a query, Google might have a record of it. *Kurtz*, 294 A.3d at 524. The affidavit includes no facts to support these speculations. As the affidavit notes, the affiant "believed" that the perpetrator "was very familiar with the victim" and that both the victim and her residence were "not randomly targeted."[44] Given these beliefs, it is just as likely, if not more so, that the perpetrator knew the victim and would *not* need to use a search engine to identify her or her house. As this Court has recognized, an "affidavit of probable cause 'must provide the magistrate with a *substantial* basis for determining the existence of probable cause[.]'" *Commonwealth v. Leed*, 186 A.3d 405, 413 (Pa. 2018) (citing *Illinois v. Gates*, 462 U.S. 213, 239 (1983) (emphasis added)). The affidavit in this case failed to do so.

Second, even if the lower court were correct that the affidavit demonstrated a "fair probability" that the warrant would uncover the identity of the individual attacker, this is insufficient to provide probable cause to support a search of an

[44] R. at 173a.

unknown number of users and their search queries.[45] *See Grossman*, 555 A.2d at 896. Under both the Fourth Amendment and Article I, Section 8, warrants must demonstrate particularized probable cause as to *every* user whose search query data is searched and seized. *Ybarra v. Illinois*, 444 U.S. 85, 91-92 (1979) ("mere propinquity" to criminal activity insufficient to establish probable cause). The keyword warrant in this case in no way approaches this requirement. Instead, it relies on what one court has called an "inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby." *United States v. Chatrie*, 509 F. Supp. 3d 901, 933 (E.D. Va. 2022); *see also id* at 928 (citing *Maryland v. Pringle*, 540 U.S. 366, 371 (2003)). Indeed, the lower court's reasoning would support a keyword warrant to Google *whenever* an officer can articulate a hunch that records of a Google search would provide evidence relevant to a criminal investigation. The keyword warrant therefore did

[45] Neither the convenience of gathering information on all individuals who searched for the phrases nor the fact that the broad warrant might return information relevant to the investigation—and might therefore be "particular" as to that information—can justify the warrant after the fact or in any event allow the introduction of that particular or particularly helpful information. *See Grossman*, 555 A.2d at 901 (although probable cause existed as to three files, warrant was overbroad because it authorized seizure of "all files").

not demonstrate "particularized probable cause" as to these users. *Chatrie*, 509 F. Supp. 3d at 929.

CONCLUSION

For the reasons stated above, this Court should reverse the lower court's decision denying Appellant's motion to suppress.

Dated: January 5, 2024

Respectfully submitted,
By: */s/ Jeremy D. Mishkin*

Jeremy D. Mishkin (PA No. 30017)
Montgomery McCracken Walker & Rhoads LLP
1735 Market Street
Philadelphia, PA 19103-7505
(215) 772-7246
jmishkin@mmwr.com

On the brief:

Andrew Crocker
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation

Daniella Gordon (PA No. 201477)
Third Circuit Vice Chair
NACDL Amicus Committee
McCarter & English, LLP
1600 Market Street, Suite 3900
Philadelphia, PA 19103
(215) 979-3812
dgordon@McCarter.com

Michael Price
Fourth Amendment Center
NACDL
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 465-7615
mprice@nacdl.org

Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers

Patrick A. Casey (PA No. 50626)
PACDL President
Myers, Brier & Kelly, LLP
425 Biden Street, Suite 200
Scranton, PA 18503
(570) 342-6100
pcasey@mbklaw.com

Attorney for Amicus Curiae Pennsylvania Association of Criminal Defense Lawyers

CERTIFICATE OF WORD COUNT COMPLIANCE

Pursuant to Pa. R.A.P. 2135, this is to certify that the Brief for Amicus Curiae Electronic Frontier Foundation complies with the word count limit set forth in Pa. R.A.P. 2135(a)(1) and 531. The word count as counted by the Microsoft Word word-processing program used to prepare this brief states that those sections that shall be included in the word count under Rule 2135(b) contain 6,940 words.

Date: January 5, 2024

/s/ Jeremy D. Mishkin
Jeremy D. Mishkin (PA No. 30017)

CONFIDENTIAL INFORMATION AND CONFIDIENTIAL DOCUMENTS CERTIFICATION

Pursuant to Pa. R.A.P. 127, 1 certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

Date: January 5, 2024

/s/ Jeremy D. Mishkin
Jeremy D. Mishkin (PA No. 30017)