IN THE SUPREME COURT OF PENNSYLVANIA

Nos. 98 MAP 2023, 99 MAP 2023, 100 MAP 2023

COMMONWEALTH OF PENNSYLVANIA

Appellee,

v.

JOHN EDWARD KURTZ

Appellant.

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION (ACLU), ACLU OF PENNSYLVANIA, LIBRARY FREEDOM PROJECT, ASSOCIATION OF RESEARCH LIBRARIES, FREEDOM TO READ FOUNDATION, AND INTERNET ARCHIVE IN SUPPORT OF APPELLANT KURTZ

Appeal from the Order of the Superior Court of Pennsylvania, 811 MDA 2021, 421 MDA 2023, and 429 MDA 2023, entered on April 28, 2023, affirming the judgement of sentence of the Northumberland County Court of Common Pleas, CP-49-CR-0000045-2018, CP-49-CR-0001236-2018, and CP-49-CR-1479-2018, entered on March 2, 2021.

Andrew Christy (Pa. I.D. 322053)
Stephen Loney, Jr. (Pa. I.D. No. 202535)
ACLU OF PENNSYLVANIA
P.O. Box 60173
Philadelphia, PA 19102
(t) 215.592.1513 x138
(f) 267.225.0447
achristy@aclupa.org

Counsel for Amici Curiae

On the brief:

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street, 7th Floor
San Francisco, CA 94104
(t) 415.343.0758

List of counsel continued on next page

Elizabeth Gyori
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, Floor 18
New York, NY 10004
(t) 212.549.2500

Matthew R. Segal
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
One Center Plaza, Suite 850
Boston, MA 02108
(t) 617.299.6664

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Other Authorities

April Glaser, *Long Before Snowden, Librarians Were Anti-Surveillance Heroes*, Slate (June 3, 2015), https://slate.com/technology/2015/06/usa-freedom-act-before-snowden-librarians-were-the-anti-surveillance-heroes.html 7

Black's Law Dictionary (10th ed. 2014) 21

Dan Roberts, *NSA surveillance: how librarians have been on the front line to protect privacy*, The Guardian (Jun. 5, 2015),.....7 https://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy

David Rudovsky, *Searches and Seizures*, *in* The Pennsylvania Constitution: A Treatise on Rights and Liberties 342, (Ken Gormley eds., 2d ed. 2020).....24

DuckDuckGo, Privacy Policy, https://duckduckgo.com/privacy.....21

Emotionalgoldmine, *ELI5: How did people "google" before Google existed?*, Reddit, https://www.reddit.com/r/explainlikeimfive/comments/3k24ua/eli5_how_did_people_google_before_google_existed.....15

Global Stats, *Search Engine Market Share*, StatCounter, https://gs.statcounter.com/search-engine-market-share..... 14, 20, 21

Google - Statistics & Facts, Statista, https://www.statista.com/topics/1001/google/#topicOverview.....15

Google, *How Google Search Works: Organizing Information*, https://www.google.com/search/howsearchworks/how-search-works/organizing-information..... 13, 14

Google, https://support.google.com/accounts/answer/9784401/..... 17

Google, https://support.google.com/a/answer/11194328 17

Google, *Privacy Policy*, https://policies.google.com/privacy?hl=en-US..... 20, 21

Herbert Mitgang, *Ideas & Trends; The F.B.I's War on Spies in the Stacks*, N.Y Times (June 26, 1988),

STATEMENTS OF INTEREST OF *AMICI CURIAE*[1]

The **American Civil Liberties Union** ("ACLU") is a nationwide, non-profit, non-partisan organization dedicated to defending the civil liberties and civil rights guaranteed by the federal and state constitutions, and the **ACLU of Pennsylvania** is the Pennsylvania state affiliate.

Library Freedom Project ("LFP") is a non-profit based in Pennsylvania which provides education and community for librarians on issues of privacy, technology, surveillance, and intellectual freedom. LFP trains librarians on these issues so that librarians may offer privacy education to their diverse communities.

The **Association of Research Libraries** ("ARL") is an association of 127 research libraries in North America. ARL's members include university libraries, public libraries, and government and national libraries. ARL programs and services promote equitable access to and effective use of recorded knowledge in support of teaching and research.

The **Freedom to Read Foundation** ("FTRF") is an organization established to foster libraries as institutions that fulfill the promise of the First Amendment; support the rights of libraries to include in their collections and make available to the public any work they may legally acquire; establish legal precedent for the

[1] No other person or entity paid for or authored this Brief.

freedom to read of all citizens; protect the public against efforts to suppress or censor speech; and support the right of libraries to collect and individuals to access information that reflects the diverse voices of a community so that every individual can see themselves reflected in the library's materials and resources.

The **Internet Archive** is a public nonprofit organization that was founded in 1996 to build an "Internet library," with the purpose of offering researchers, historians, scholars, artists, and the general public permanent access to historical collections in digital format. The Internet Archive then provides free public access to its data—which include text, audio, video, software, and archived web pages.

INTRODUCTION

This case involves a novel surveillance technique. The police obtained records reflecting everyone who used Google's Search tool to seek information related to a particular word or phrase—in this case, a home address—within a defined time period. This is called a "reverse search." Instead of seeking information about an identified suspect, a reverse search seeks to identify suspects by demanding that a company comb through its huge repository of data reflecting the public's

interactions with its services. Even when it identifies suspects, this technique traps countless innocent people in its net.

In this case, the lower court approved a reverse search seeking Google Search history records that would reveal the identity of anyone who queried for a particular address at a particular point in time. It concluded that no individual maintains a reasonable expectation of privacy at all in *any* query they enter into a search engine—whether it's an address, a name, a topic, or an idea. This view, if upheld, would provide the police with unfettered access to the thoughts, feelings, concerns, and secrets of countless people, simply because they enter those thoughts, feelings, concerns, and secrets into third-party-operated search engines that have become indispensable features of modern life.

Amici include First Amendment advocacy groups, librarians, and librarian-led organizations familiar with the privacy protections that apply to another type of information-access records: library patron records, traditionally the materials that patrons borrow under their names. Given the sensitivity of these records, every state mandates that they remain private, and librarians take pains to safeguard them. This brief compares and contrasts borrowing histories with Internet search queries, which are even more detailed, revealing, and persistent than library records. Society expects library records to be kept private. Internet search histories therefore must be far more protected because they are far more revealing.

Because of that, both Article 1, Section 8 of the Pennsylvania Constitution and the Fourth Amendment to the U.S. Constitution protect search query data. Moreover, because of the obvious First Amendment interests implicated by government access to these records, those constitutional provisions must be applied with "scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 565 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). The Superior Court therefore erred in holding that search queries receive no constitutional protection.

ARGUMENT

I. Library practices and legal protections demonstrate that individuals reasonably expect that records of their information searches are private.

Being able to search for information and receive answers is protected by the Constitution. *Stanley v. Georgia*, 394 U.S. 557, 564 (1969). It is now well established that the Constitution protects the right to receive information and ideas. 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 Martin v. City of Struthers*, 319 U.S. 141, 146-47 (1943) ("Freedom to distribute information to every citizen wherever he desires to receive it is so clearly vital to the preservation of a free society that . . . it must be fully preserved."). 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." *Board of Educ.*, 457 U.S. at 867 (second emphasis added).

It is through listening to others that "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).

A. Library policies and practices reflect society's longstanding commitment to intellectual privacy.

Before there were search engines to access the Internet, there were physical libraries to access printed and other information. And while society has long considered library records to be private and treats them as such, they are far less revealing than the kind of search engine records implicated by this case, indicating that search histories deserve even more protection than traditional book borrowing records. Privacy has been a core value of librarianship for almost one hundred years.[2] Librarians, including *Amici*, recognize the relationship between intellectual freedom and privacy—people cannot read, write, or research freely if they fear surveillance, which motivates self-censorship. The very purpose of libraries is bound up in a foundational respect for the privacy of individual inquiry into the world.

Libraries have a long history of protecting patrons' intellectual privacy against government overreach. In the early 1970s, librarians resisted attempts by the federal government to access patron borrowing records as part of broad investigations against left wing radicals. Steve Witt, *The Evolution of Privacy within the American*

[2] American Library Ass'n, Code of Ethics (1939), https://www.ala.org/tools/ethics.

Library Association, 1906-2002, 65 Library Trends 639, 651–652 (2017). Later in that decade, librarians resisted the FBI's Library Awareness Program, a clandestine counterintelligence effort intended to monitor which books Soviet bloc immigrants were checking out of public libraries.[3]

Librarians were also quick to adapt to new threats to privacy posed by technological change. After 9/11, the American Library Association responded in various ways to the federal government's attempts to unlawfully and secretly surveil patron borrowing habits through Section 215 of the PATRIOT Act, also known as the library records provision.[4] Librarians then implemented a new default practice to completely delete patron checkout histories once materials were returned, a practice that has remained a standard feature in all library checkout software around

[3] Herbert Mitgang, *Ideas & Trends; The F.B.I's War on Spies in the Stacks*, N.Y Times (June 26, 1988), https://www.nytimes.com/1988/06/26/weekinreview/ideas-trends-the-fbi-s-war-on-spies-in-the-stacks.html.

[4] American Library Ass'n, USA Patriot Act: A Summary of ALA Activities (Jan. 19, 2022), (prepared for a workshop on the USA Patriot Act) https://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/background.pdf; American Library Ass'n, Resolution On The USA Patriot Act And Related Measures That Infringe On The Rights Of Library Users (Jan. 29, 2003), https://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/alaresolution.htm; American Library Ass'n, *The USA Patriot Act and Libraries*, *in* The State of America's Libraries, 9-11 (2006), https://www.ala.org/ala/pressreleases2006/march2006/4-06_StateofAmericasLibraries.pdf.

the country.[5] Today, librarians continue to support privacy and free expression by teaching the public how to protect their privacy, and by strengthening privacy protections in library policies and systems.[6]

Libraries are also among the few public spaces where people from all walks of life interact, so librarians have a unique awareness of how the loss of privacy affects different communities. For example, senior citizens and others with lower technical skills can have their identities stolen or be victims of fraud.[7] LGBTQ people, especially young people, can be "outed" to hostile communities and risk losing work, housing, or educational access.[8] Domestic violence victims can have

---

[5] Sam Thielman, *You Are Not What You Read: Librarians Purge User Data To Protect Privacy*, The Guardian (Jan. 13, 2016), https://www.theguardian.com/us-news/2016/jan/13/us-library-records-purged-data-privacy; April Glaser, *Long Before Snowden, Librarians Were Anti-Surveillance Heroes*, Slate (June 3, 2015), https://slate.com/technology/2015/06/usa-freedom-act-before-snowden-librarians-were-the-anti-surveillance-heroes.html.

[6] Zoe Carpenter, *Librarians Versus the NSA*, The Nation (May 6, 2015), https://www.thenation.com/article/archive/librarians-versus-nsa; Dan Roberts, *NSA surveillance: how librarians have been on the front line to protect privacy*, The Guardian (Jun. 5, 2015), https://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy; American Library Ass'n, State of America's Libraries, 11 (2023), https://www.ala.org/news/sites/ala.org.news/files/content/state-of-americas-libraries-report-2023-web-version.pdf; Library Freedom Project, https://libraryfreedom.org.

[7] Steven Kemp & Nieves Erades Perez, *Consumer Fraud against Older Adults in Digital Society: Examining Victimization and Its Impact*, 20 Int'l J. of Env't Rshc. and Pub. Health 5404, 5405 (2023).

[8] Michelle Forrest, *For LGBTQ Youth, Truly Equitable Internet Access Requires End-to-End Encryption*, New America Found.: Open Technology Inst. Blog (Jan.

information about their location revealed to abusers.[9] Health data leaked without consent can lead to employment or insurance discrimination, or even social ostracization.[10]

Librarians have unique insight into the importance of privacy for individuals who are searching for information. The work that librarians undertake to safeguard patron records reflects society's longstanding recognition that records reflecting people's information-seeking activities deserve privacy protections.

B. Positive law has long recognized that library patrons have a privacy interest in records reflecting their efforts to access information.

Since library records—like Internet search engine records—can reveal deep and intimate information about patrons' interests, desires, and personhood, every state has enshrined in law some form of privacy protections. In assessing whether an expectation of privacy is objectively reasonable, "prevailing rules in individual jurisdictions" and the trend in relevant state laws are relevant considerations. *Tennessee v. Garner*, 471 U.S. 1, 15–18 (1985) (citing *United States v. Watson*, 423

28, 2022), https://www.newamerica.org/oti/blog/for-lgbtq-youth-truly-equitable-internet-access-requires-end-to-end-encryption/.

[9] Safety Net Project, https://www.techsafety.org/privacymatters.

[10] Inst. Of Medicine, Comm. on Health Rsch. and Priv. of Health Info.: The HIPAA Priv. Rule, Beyond the HIPAA Privacy Rule, *Enhancing Privacy, Improving Health Through Research* 80 (Nass SJ et al. eds., 2009).

U.S. 411, 421–22 (1976)); *see also Florida v. Riley*, 488 U.S. 445, 451 (1989) (plurality opinion).

Forty-eight states and the District of Columbia have at least one statute, if not more, protecting the confidentiality of library patron records.[11] The other two states—Kentucky and Hawaii—have longstanding Attorney General Opinions that similarly protect library records.[12] Of the 58 total legal protections for library records, 47 affirmatively prohibit any disclosure unless certain requirements are met while 11 exempt the records from required disclosure pursuant to a state's public records law.[13] In 37 states and the District of Columbia, these protections mandate that a party seeking to access library patron records obtain a court order to do so.[14] While a subpoena is most often deemed as an acceptable court order under these statutes, four statutes explicitly state that a warrant is adequate for compelled disclosure.[15]

---

[11] *See* Ex. A at 1-2.
[12] *See* Ex. A at 1. Further, Hawaii's protections are enshrined in its administrative code. *See* Haw. Admin. R. § 8-200.5-3.
[13] *See* Ex. A at 1-2. As shown in Ex. A, five states (AR, MD, NH, RI, UT) have two or more different statutes protecting library records from disclosure while Hawaii protects records through an Attorney General Opinion and its administrative code. For assessing reasonable expectations of privacy, the Court looks to the rules governing public access to private information or areas, rather than to what law enforcement can do. *See California v. Ciraolo*, 476 U.S. 207, 213–14 (1986); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1825–26, 1831 (2016).
[14] *See* Ex. A at 3-4.
[15] *Id*.

Pennsylvania is in the majority of states whose laws explicitly require a court order before libraries may disclose patrons' records. Pennsylvania law mandates that "[r]ecords . . . which relate to the circulation of library materials and contain the names or other personally identifying information of users of the materials shall be confidential and may not be made available to anyone except by a court order in a criminal proceeding." 24 Pa.C.S. § 9375. The only procedure set forth in Pennsylvania law that would allow law enforcement to obtain such a court order for library records is to obtain a search warrant pursuant to Pa. R. Crim. P. 203.[16] Under that rule, "[n]o search warrant shall issue but upon probable cause supported by one or more affidavits sworn to before the issuing authority in person or using advanced communication technology." Pa. R. Crim. P. 203(B). Accordingly, Pennsylvania law protects access to library records with the highest constitutional standard.

Thus, states that otherwise disagree on many asserted freedoms—from gambling to hunting to firearms—broadly agree that library patron records deserve special legal protection. This judgment, expressed by states and legislatures across the country, reflects society's understanding that people have a privacy interest in the interests, beliefs, fears, secrets and other critical aspects of personhood that they may divulge when seeking information at libraries.

[16] There is no Rule that authorizes the issuance of subpoenas in criminal investigations.

To be sure, many of these same states allow law enforcement to, under certain circumstances, obtain library records using a subpoena rather than the probable-cause warrant required in Pennsylvania. But even states that do not require warrants support the conclusion that the privacy expectations for information divulged when people use libraries merit constitutional protection. And, for three reasons, the procedures used to subpoena library records reflects society's recognition of the robust privacy interests at stake.

First, in practice, the subpoena process at libraries has often provided even more privacy protections than in response to a warrant because it typically allows libraries to consult with legal counsel and carefully select the records that are being sought, while limiting needless disclosures. *See, e.g.*, *Rothman v. Court of Common Pleas of Dauphin Cnty.*, 564 A.2d. 912, 912–13 (Pa. 1989) (subpoena gave responding party time in which to comply or challenge the subpoena); *Commonwealth v. Stewart*, 690 A.2d 195, 196–98 (Pa. 1997) (same). A library can also move to quash a subpoena it regards as improper, which allows an impartial court to determine its legality. *See*, *e.g.*, *Rothman*, 564 A.2d at 912-13. Libraries are well-situated to serve in this patron-protecting role, without undermining true law enforcement needs, because as government agencies, they are presumed to act in good faith. *See Commonwealth, Office of Governor v. Donahue*, 98 A.3d 1223, 1239 (Pa. 2014); *Belmont Abbey Coll. v. Sebelius*, 878 F.Supp.2d 25, 36 (D.D.C. 2012)

(citing *Comcast Corp. v. F.C.C.,* 526 F.3d 763, 769 (D.C. Cir. 2008); *Adair v. England,* 183 F.Supp.2d 31, 60 (D.D.C. 2000).[17]

Second, subpoenas must state with particularity the records sought, so that executing agencies avoid acquiring extraneous information. Under the Fourth Amendment, subpoenas must be reasonable, meaning that they may not be overly broad or indefinite. *See Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946); *United States v. Morton Salt Co.*, 338 U.S. 632, 652–53 (1950); *United States v. Powell*, 379 U.S. 48, 57–58 (1964). Subpoenas must also seek relevant information, be properly issued, and be for a legitimate purpose. *See McLane Co., Inc. v. E.E.O.C.*, 581 U.S. 72, 76–77 (2017), *as revised* (Apr. 3, 2017); *Univ. of Penn. v. E.E.O.C.*, 493 U.S. 182, 191 (1990); *Powell*, 379 U.S. at 57–58.

Third, many court orders allow the person or entity that is the subject of the order to challenge the disclosure for its failure to comply with the Fourth Amendment, ensuring protections against needless privacy invasions. *See*, *e.g.*, *Commonwealth v. Mucci*, 143 A.3d 399, 412 (Pa. Super. Ct. 2016) (upholding trial court's order to quash a subpoena because it was overly broad). These protections, in tandem, have created an ecosystem in which library patrons reasonably believe that they enjoy robust privacy protections when searching for information.

[17] State-based subpoena processes also resemble the procedures by which *warrants* protect private communications under the Stored Communication Act. *See* 18 U.S.C. § 2703(a); *infra.* pp 22-23.

II. Search query records differ from library records in both a quantitative and a qualitative sense, making them even more deserving of constitutional protections.

Today, librarians assist patrons in accessing online and digital resources that reach well beyond the books and periodicals of old. Like library records, online search histories capture intimate and profound details about one's personhood. But search records are vastly more revealing than traditional library patron records because they combine huge databases, intelligent search process, and search results based on sensitive personal information that a user includes in a query.

A. Using a search engine is unavoidable and search histories are extensive.

Internet searches have become a natural and nearly automatic way for people to acquire information because they are gateways to the Internet and because the results they produce are extremely useful. Internet searches draw upon larger and different repositories than the searches that occur within libraries' physical spaces. Consider Google. Its virtual collection, called Index, "contains hundreds of billions of webpages and is well over 100,000,000 gigabytes in size."[18] That is enough to cover 40 billion books averaging 300 pages in length—i.e., more books than any

[18] Google, *How Google Search Works: Organizing Information*, https://www.google.com/search/howsearchworks/how-search-works/organizing-information.

physical library has ever contained.[19] But, of course, Google is not limited to books.[20] The Index includes, among other things: reference works like Wikipedia; social media; over one billion YouTube videos;[21] and image collections.[22]

Without search engines, it is nearly impossible to navigate this sea of information. Even if the user already knows which web site they want to access, web site addresses—uniform resource locators or URLs—are often too long to memorize.[23] If a user wants to buy a print of Claude Monet's "Impression: Sunrise" on Art.com, they could try to memorize a webpage URL like "https://www.art.com/products/p14498961582-sa-i6740557/claude-monet-impression-sunrise-1872.htm." Or they could Google it.

That is why so many people use search engines. As of February 2023, Google, the dominant search engine worldwide and in the United States[24], has 274.49 million

---

[19] *See* Library of Congress, Fascinating Facts, https://www.loc.gov/about/fascinating-facts/# (noting that the Library of Congress is the world's largest library with millions of items).
[20] Google, *supra* note 16.
[21] Prashant Sharma, *How Many Videos Are on YouTube: Exploring the Vast Digital Landscape*, TechPluto (July 5, 2023), https://www.techpluto.com/how-many-videos-are-on-youtube/#How_Many_Videos_Are_There_on_YouTube/.
[22] *Id.*
[23] *See* Katie Dean, *Ooooh, That URL Is Ugly!*, Wired (Oct. 13, 1999), https://www.wired.com/1999/10/ooooh-that-url-is-ugly.
[24] Global Stats, *Search Engine Market Share*, StatCounter, https://gs.statcounter.com/search-engine-market-share.

unique visitors in the United States,[25] which accounts for 83% of the total population[26] and about 90% of all Internet users.[27] Google processes 99,000 search queries every second.[28] The average user conducts more than three Google searches per day.[29] For some people, Internet searches are the only form of research they have ever known.[30] It is fair to say that search engines are "'such a pervasive and insistent part of daily life' that [using] one is indispensable to participation in modern society." *United States v. Carpenter*, 138 S. Ct. 2206, 2220 (2018) (citing *Riley v. California*, 573 U.S. 373, 385 (2014)) (comparing the world before cell phones where a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy with the modern world where people carry immense amounts of data with them).

---

[25] *Google - Statistics & Facts*, Statista, https://www.statista.com/topics/1001/google/#topicOverview.
[26] *U.S. and World Population Clock*, United States Census Bureau, https://www.census.gov/popclock.
[27] *Internet Usage in the United States – Statistics & Facts*, Statista, https://www.statista.com/topics/2237/internet-usage-in-the-united-states/#editorsPicks.
[28] Torbjørn Flensted, *How Many People Use Google? Statistics & Facts (2023)*, SEO AI Blog (Sep. 1, 2023), https://seo.ai/blog/how-many-people-use-google#.
[29] *Id.*; Lily Ray, *We Surveyed 1,400 Searchers About Google – Here's What We Learned*, Moz Blog (Apr. 19, 2019), https://moz.com/blog/new-google-survey-results (surveying Google users and finding that 77% of respondents search on Google more than three times a day).
[30] Emotionalgoldmine, *ELI5: How did people "google" before Google existed?*, Reddit, https://www.reddit.com/r/explainlikeimfive/comments/3k24ua/eli5_how_did_people_google_before_google_existed.

Moreover, online search history records are more voluminous than library patron records. Library records will show which materials a patron has checked out or has put on hold. But third-party businesses that run search engines log Internet users' queries, creating digital trails that years ago would have never existed, except as a private memory. What is more, these logs are created numerous times per day, since the ability to quickly and frequently search the Internet is in almost everyone's pocket.

B. Online search histories are highly revealing.

Search engines make this vast library of information useable by recording the users' unique and specific search queries. Traditionally, library patrons look for physical materials using broad categories like the author's name, the work's title, or a topic assigned by a third party. If someone wants to research whether they are over- or under-weight, they may well be able to find relevant books about health. Reviewing the indices of the books for topics like "weight" or "body mass index" can direct the reader to pages containing charts of average weights and heights. The patron may read this information for a few second or a few hours. A library-records subpoena will reveal at most that this person checked out a health-related book.

Internet searches are far more targeted and detailed. If someone Googles "is 250 pounds overweight for 6 feet?" they will have the convenience of instantly seeing the answer highlighted on the results page, as well as helpful links to BMI

calculators, weight loss tips to click on, and ads for products to buy.[31] But, unlike the library, Google also will have an record apparently reflecting the person's height, weight, and evidence of their concern that they might be fat.

As the above example shows, Internet users get the most useful search results by revealing detailed sensitive information about themselves. Search engines routinely retain user search histories in order to generate user-specific results.[32] For Google users logged into their accounts, Google stores their search histories alongside their identifying information, as well as all browsing histories: websites they visited, videos played, songs streamed, social media posts viewed and liked.[33] Google allows people to delete their search histories, either manually or automatically. But by default, it currently retains this data for 18 months—thousands or tens of thousands of searches.[34] For these reasons, while Internet search histories are akin to patrons' library records, law enforcement access to them is a far greater privacy invasion by orders of magnitude.

---

[31] *See* Google, https://www.google.com/search?q=is+250+pounds+overweight+for+6+feet

[32] Sundar Pichai, *Keeping your private information private*, Google: Blog, https://blog.google/technology/safety-security/keeping-private-information-private (implementing auto-deletion for app search activities after 18 months for accounts created after 2020 and providing the option for earlier accounts).

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

[34] Google, https://support.google.com/accounts/answer/9784401/; Google, https://support.google.com/a/answer/11194328.

Moreover, Internet searches can operate in combination to paint a detailed profile of the user's medical diagnoses, religious beliefs, financial stability, sexual desires, relationship status, family secrets, political leanings, and more.[35] For example, a study in 2019 found that 89% of U.S. citizens search their health information online before seeking medical care.[36] That is, before seeing a doctor about a physical symptom or a possible mental illness, an Internet user would Google it. Those searches may be enormously helpful; they might even spur someone to seek life-saving care.

But they will also create a deeply revealing digital trail. Even when Google users refrain from logging in, they cannot completely prevent Google from creating records of their search histories. In that circumstance, searches are still retained, and the search engine can identify the searcher through their IP addresses and Internet service provider. On major search engines like Google and Bing, the only way to avoid leaving a digital trail is to avoid searching the Internet—or possibly to avoid using the company's Internet browser *at all*.[37]

---

[35] Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU News & Commentary (Nov. 12, 2023), https://www.aclu.org/news/national-security/how-private-your-online-search-history.
[36] Alex Guarino, *Study Finds 89% of US Citizens Turn to Google Before Their Doctor*, WECT (June 24, 2019), https://www.wect.com/2019/06/24/study-finds-us-citizens-turn-google-before-their-doctor.
[37] *Id.*

To be sure, libraries have historically kept aggregated records on the materials their patrons check out. But conversations with librarians are not recorded, libraries allow anonymous computer usage, and some libraries do not keep search records at all.[38]

In practice, this means Internet searches demand that users reveal more about themselves than they do when searching physical materials at libraries. A library patron can ask a librarian for a book explaining how late someone's menstrual period can begin if they are not pregnant. The patron might then read that book and look up the local Planned Parenthood in the Yellow Pages, all without creating a written record of any kind. Not so on the Internet. If an Internet user searches "how late can a missed period be," and then searches "Planned Parenthood," they will leave an unmistakable and deeply person digital trail. In some states where abortion is now a crime, those searches may be evidence. And yet, under the lower court's reasoning, investigators could warrantlessly demand that Google identify *everyone* who searched for "Planned Parenthood."

[38] *See e.g.*, New York Public Library, *How can I see the books I've borrowed?*, https://libanswers.nypl.org/faq/364130.

III. The way companies handle search history justifies the belief that the data is private.

A. Providers assure users that their search histories are confidential.

Internet users reasonably expect that their search queries are private in part because that's what search engine companies tell them. Every search engine treats the data as belonging to the user, and not to the company.

Google, the dominant search engine and the one police searched here, retains user search histories, but pledges that it "do[es] not share [the user's] personal information with companies, organizations, or individuals outside of Google."[39] The company requires a specific and narrowly tailored warrant in order for it to reveal information connected to the alleged crime under investigation.[40]

Microsoft's Bing, the next largest search engine, promises that the user is "in control of the search history associated with [their] personal Microsoft account."[41] DuckDuckGo does not record, and thus cannot share, users' search or browsing

[39] Google, *Privacy Policy*, https://policies.google.com/privacy?hl=en-US.
[40] *See Declaration of Legal Investigations Support Analyst Nikki Adeli* at 3, *People v. Seymour*, 2021-CR-20001 (Colo. Dist. Ct., 2022) (June 5, 2023) https://www.nacdl.org/getattachment/13d9ccb1-5e6d-4dfd-a8e2-57c32fafbc2d/google-declaration-of-nikki-adeli.pdf.
[41] Statcounter, *supra* note 22; Microsoft, *How Microsoft Search in Bing helps keep your info secure*, https://support.microsoft.com/en-au/office/how-microsoft-search-in-bing-helps-keep-your-info-secure-cbce46ae-bb1f-4d0e-86f1-5984f4589113

history.[42] Both Google and Bing allow users to delete their search histories.[43] Both assure users that the company will not reveal their data to law enforcement unless the company believes it is *necessary* to release that information in order to comply with a request that meets the necessary legal standards.[44]

The users, in other words, retain a possessory interest in their search history data—the "right to control property, including the right to exclude others, [even] by a person who is not necessarily the owner." Black's Law Dictionary (10th ed. 2014) (emphasis added); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."). Users protect their accounts with passwords. Providers encrypt user emails both in transit and when stored on servers in order to exclude outsiders. Users also have the right to delete their email messages or other online data. Because search histories are treated as personal property, they are protected by the Constitution from unreasonable searches and seizures. Courts have considered and rejected arguments to the contrary. *See, e.g., United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) ("While . . . a

[42] Statcounter, *supra* note 22; DuckDuckGo, Privacy Policy, https://duckduckgo.com/privacy.
[43] Microsoft, https://support.microsoft.com/en-us/topic/turn-search-history-off-or-on-b0f77f8c-5235-4bea-93a7-c93733329979.
[44] *Privacy Policy*, Google, *supra* note 37; Microsoft, *Microsoft Privacy Statement*, https://privacy.microsoft.com/en-us/privacystatement.

subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . we doubt that will be the case in most situations . . . ."); *United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (policies establishing limited instances of access do not vitiate Fourth Amendment interests).

Users reasonably rely on the companies' representations when expecting a privacy and property interest in their search histories.

B. The Stored Communications Act requires a warrant for search history data, indicating that the information receives the highest privacy protections.

The warrant requirements of the federal Stored Communications Act ("SCA") also support a conclusion that people reasonably expect their search histories to be treated as private. The SCA prohibits providers of "electronic communication services" ("ECS") from voluntarily providing the contents of electronic communications to the government. 18 U.S.C. § 2702(a)(1). The definition of ECS encompasses search engines because it includes services that allow users "to send or receive wire or electronic communications,". 18 U.S.C § 2510(15).

If law enforcement wants to obtain information from an ECS, it must compel disclosure through appropriate legal process. The exact rules are complicated. *Konop v. Hawaiian Airlines Inc.*, 302 F.3d 868, 874 (9th Cir. 2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003) (agreeing). But as a general matter, the SCA

requires law enforcement to get a warrant to obtain content from an ECS. 18 U.S.C. § 2703(a). There are no courts that have held that law enforcement may constitutionally acquire noncontraband digital content without a warrant under the SCA.

IV. The Pennsylvania and U.S. Constitutions protect the public's expectation of privacy in search history data.

The Pennsylvania and United States Constitutions protect people against unreasonable searches and seizures. Pa. Const. art. 1 § 8; U.S. Const. amend. IV. These protections safeguard the privacy and security of individuals against arbitrary invasions by governmental officials, including intrusions that involve the government's acquisition of information. *See, e.g., Commonwealth v. Edmunds*, 586 A.2d 887, 897 (Pa. 1991) ("At the time the Pennsylvania Constitution was drafted in 1776, the issue of searches and seizures unsupported by probable cause was of utmost concern to the constitutional draftsmen."); *Katz v. United States*, 389 U.S. 347 (1967); *United States v. Jones*, 565 U.S. 400 (2012). Given the longstanding protections for information-gathering that occurs at libraries, and that online information-gathering is even more sensitive than that which occurs at libraries, state and federal Constitutions protect the privacy interests here with a warrant.

A. The Pennsylvania Constitution protects search query information.

The Superior Court's ruling in this case rests on the notion that Internet users lack constitutionally cognizable privacy interests in their search queries because the

queries are sent to third-party search engines like Google and Bing. But, in interpreting Article I, Section 8, of the Pennsylvania Constitution, this Court has rejected the federal "third-party doctrine", calling it "a dangerous precedent, with great potential for abuse." *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979). As noted in the leading treatise on the Pennsylvania Constitution, this Court has instead "give[n] the reasonable expectation of privacy concept robust interpretation," even as the U.S. Supreme Court has weakened it.[45] A robust interpretation of Article I, Section 8, is particularly warranted in the context of Internet searches.

It is important to start with the reasons why this Court has rejected the federal third-party doctrine. In its ruling on bank records in *DeJohn*, the Court understood the reality of participating in modern society: "For all practical purposes," providing information to third-party corporations "is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." *DeJohn*, 403 A.2d at 1289 (quoting *Burrows v. Superior Court of San Bernadino County*, 529 P.2d 590, 596 (Cal. 1974)). It accordingly rejected the "simplistic propriety analysis" used by the U.S. Supreme Court in *United States v. Miller*, 425 U.S. 435 (1976), where the Court held there

[45] David Rudovsky, *Searches and Seizures*, *in* The Pennsylvania Constitution: A Treatise on Rights and Liberties 342, (Ken Gormley eds., 2d ed. 2020).

was no expectation of privacy in bank records. *DeJohn*, 403 A.2d at 1290. Rather, the Pennsylvania Court adopted an analysis that "recogniz[es] modern electronic realities." *Id.* The Court recognized, in particular, the reality that private corporations now provide services that are necessary for society to function and individuals to participate in modernity.

Significantly, while the Court also recognized that a person does "to a limited extent" lose a reasonable expectation of privacy by writing information on the face of a check, that loss is limited to the scope and duration of *one* financial transaction—instead of deeming that loss of privacy to *permanently* and *forever* follow the writer of the check. *DeJohn*, 403 A.2d 1290 ("We believe that the drawer of a check, to a limited extent, gives up his right to privacy in that check *while that check is circulated in commercial channels*." (emphasis added)). The Court also indicated that any diminishment of privacy was not only fleeting but also limited to "the information contained in *a single* negotiable instrument." *Id.* Importantly, for purposes of applying this decision in the context of search engines like Google and Bing, the Court did not say that a bank customer loses a privacy interest in the *aggregate* of all information that might appear in "the bank's retention of a record of such disclosures." *Id*. at 1291 (quoting *Burrows*, 529 P.2d at 592).

Since *DeJohn*, this Court has continued to reject the broad third-party doctrine as incompatible with the Pennsylvania Constitution. *See*, *e.g.*, *Commonwealth v.*

Melilli, 555 A.2d 1254, 1258-59 (Pa. 1989) (holding that a warrant supported by probable cause is required to install a pen register, a device recording the phone numbers called by a person, due to privacy rights); *Commonwealth v. Duncan*, 817 A.2d 455, 451-452 (Pa. 2003) (permitting the government to obtain the name and address of a bank customer without a warrant because the name and address do not "reveal anything concerning his personal affairs, opinions, habits or associations"). This jurisprudence recognizes that *substantive* personal information—about a person's spending, communications, views, habits, opinions, religion, politics, etc.—does not lose state constitutional protection just because that information could be gleaned from unavoidable transactions that the person undertakes with third parties. And the logic of those cases applies, with special force, to the Internet searches at issue here.

As shown above, Internet searches can reveal private medical decisions, political views, religious affiliations, and more, providing an unparalleled view of a person's most private and intimate life. Internet searches are now by far the most practical way to find doctors and health care, houses of worship, political organizations, or even social groups and romantic partners. Phonebooks are a relic of the past; the Internet is what people rely on, and the necessity of using the Internet is that private corporations know what people search. No person using the Internet believes that the government will access all of this private information at will.

Instead, Article I, Section 8 provides the proper balance between that entirely reasonable expectation of privacy in the fundamental privacy rights of Pennsylvanians, by ensuring that the government can learn these intimate details only if it obtains a warrant based on probable cause.

It is no answer to say that some Internet users may understand that Google and Bing retain information about them. Under *DeJohn*, any diminishment of privacy in a Google search is limited in duration to the vanishingly brief time that elapses "while" Google runs the query against its Index. 403 A.2d at 1290. And unlike in *DeJohn*, where there was at least an argument that actual human beings "may see a customer's checks in bundles," *id.* at 1291, an Internet user has no reason to believe that any human being ever reviews what they type into a search bar.

Here, the lower court erred for an additional reason when it found no expectation of privacy in the defendant's IP addresses. It considered the privacy of IP addresses associated with search queries *separately* from an individual's privacy interests in his or her search history records. While a number of courts have held that there is no expectation of privacy in IP addresses *alone*, the IP addresses here were part and parcel of the search history records—one of several columns on a spreadsheet. When IP address or similar data are indivisible from the other data points in a record and the record as a whole is private, sensitive, and revealing, the Constitutions protect all the data contained in those records.

Thus, the Superior Court's reasons for rejecting an expectation of privacy simply have no traction under this state's Constitution.

B. The Fourth Amendment to the U.S. Constitution protects search query information.

Although this Court can resolve this case under the Pennsylvania Constitution alone, the Superior Court's ruling also runs afoul of the Fourth Amendment because it overextends the federal third-party doctrine as recently narrowed by the U.S. Supreme Court. In a series of cases addressing the power of "technology [to] enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (*quoting Kyllo v. United States*, 533 U.S. 27, 34 (2001) (last alteration in original)); *accord Jones*, 565 U.S. at 406. As Justice Alito explained in *Jones*, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." 565 U.S. at 429 (Alito, J., concurring in judgment).

To this end, the Court has pointed to Internet search and browsing history as a type of data that is "qualitatively different" from transactional data shared with third parties. *Riley*, 573 U.S. at 373 (2014). In this context, the Court noted that "Internet search and browsing history can be found on an Internet-enabled phone

and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Id*. at 395.

A few years later, the Court held that non-content cell phone location data is protected with a warrant requirement even when held by third parties. *See Carpenter*, 138 S. Ct. at 2217–18; *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment); *id.* at 415–16 (Sotomayor, J., concurring). As the Court highlighted in the context of location data generated from the use of a cell phone, when a "newfound tracking capacity runs against everyone," and "[o]nly the few without cell phones could escape this tireless and absolute surveillance," the Fourth Amendment applies. *Carpenter*, 138 S. Ct. at 2218. The Court in *Carpenter* also distinguished the cell phone location information at issue in that case from traditional law enforcement surveillance on the basis of "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id.*

That reasoning applies even more strongly to search history records. Both cell phones and Internet searches are "indispensable to participation in modern society." *Id.* at 2220. And, as explained above, using search engines is just as pervasive, and as a practical matter just as unavoidable, as using a cell phone. Indeed, search histories reveal categories of information going far beyond location, and far more extensive even than library records, at a volume and specificity akin to mind reading. The confluence of these factors—detailed, indiscriminate, and pervasive data

collection on *content*—explains why the Superior Court was wrong to conclude that people have no expectation of privacy in their search history records.

The Superior Court purported to rely on Google's privacy policy, which it inaccurately described as "specifically allow[ing] for the company to turn over search results when *requested* by law enforcement." *Commonwealth v. Kurtz*, 294 A.3d 509, 522 (Pa. 2023). In fact, Google's privacy policy makes clear that it will not comply with a law enforcement request unless it has a good faith belief that disclosure is *necessary* to comply with a request that meets the applicable legal standards. Google, *supra* note 39. Regardless, the U.S. Supreme Court has consistently declined to base its account of a person's privacy rights against *government* intrusion on the terms of that person's business relationships with a *private* company. *See Carpenter*, 138 S. Ct. 2206 (resolving case without relying on cell phone provider's terms of service); *United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018) (resolving case about privacy expectation in a rental car despite rental car agreement).

What is more, unlike *Carpenter*, the government's acquisition of individuals' Internet search queries involves the direct acquisition of the *content* of communications, messages that reveal their substance, purport, or meaning. 18 U.S.C. § 2510(8). Every Justice of the Supreme Court has suggested that the Fourth Amendment protects the content of digital documents stored with third parties. *See*

Carpenter, 138 S. Ct. 2206 at2222 (2018) (majority op.) ("If the third-party doctrine does not apply to the 'modern-day equivalents of an individual's own 'papers' or 'effects,'' then the clear implication is that the documents should receive full Fourth Amendment protection."); *id* at 2230 (Kennedy, J., dissenting) (discussing "'papers' or 'effects' even when those papers or effects are held by a third party"); *id* at 2262, 2269 (Gorsuch, J., dissenting) (stating that "no one believes" the Court's third-party doctrine cases should be construed to allow review of private documents held by third parties).

If adopted by this Court, the lower court's reasoning would undermine fundamental privacy protections in communication media used by nearly all Americans and disrupt current established practice for access to personal information stored online, including search histories.

CONCLUSION

For these reasons, this Court should reverse the lower court and hold that search history data is protected by the state and federal Constitutions.

Dated January 10, 2024

Andrew Christy (Pa. I.D. 322053)

Stephen Loney, Jr. (Pa. I.D. No. 202535)
ACLU OF PENNSYLVANIA
P.O. Box 60173

Philadelphia, PA 19102
(t) 215.592.1513 x138
(f) 267.225.0447
achristy@aclupa.org
Counsel for Amici Curiae

On the brief:

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street, 7th Floor
San Francisco, CA 94104
(t) 415.343.0758

Elizabeth Gyori
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, Floor 18
New York, NY 10004
(t) 212.549.2500

Matthew R. Segal
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
One Center Plaza, Suite 850
Boston, MA 02108
(t) 617.299.6664

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the word-count limits of Pa.R.A.P. 531, as it contains fewer than 7,000 words, exclusive of excluded materials.

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

Dated January 10, 2024

/s/ Andrew Christy
Andrew Christy, Pa. I.D. 322053
ACLU OF PENNSYLVANIA
P.O. Box 60173
Philadelphia, PA 19102
(t) 215.592.1513 x138
(f) 267.225.0447
achristy@aclupa.org
Counsel for Amici Curiae

EXHIBIT A

Analysis of State Protections for Patrons' Library Records

Chart of State-by-State Legal Protections for Patrons' Library Records

State	Statute/Code/Opinion	Type of Prohibition
AL	Ala. Code § 41-8-10	Disclosure prohibited
AK	Alaska Stat. Ann. § 40.25.140	Disclosure prohibited
AZ	Ariz. Rev. Stat. Ann. § 41-151.22	Disclosure prohibited
AR	Ark. Code Ann. § 13-2-704	Disclosure prohibited
AR	Ark. Code Ann. § 13-2-706	Disclosure prohibited
CA	Cal. Gov't Code Ann. § 7927.105	Disclosure prohibited
CO	Colo. Rev. Stat. Ann. § 24-90-119	Disclosure prohibited
CT	Conn. Gen. Stat. Ann. § 11-25	Disclosure prohibited
DE	Del. Code Ann. tit. 29, § 10002(o)(12)	Exempts from mandatory public records disclosure
DC	D.C. Code Ann. § 39-108	Disclosure prohibited
FL	Fla. Stat. Ann. § 257.261	Disclosure prohibited
GA	Ga. Code Ann. § 24-12-30	Disclosure prohibited
HI	Attorney General Op. Ltr. 90-30 (on file)	Exempts from mandatory public records disclosure
HI	Haw. Admin. R. § 8-200.5-3	Disclosure prohibited
ID	Idaho Code Ann. § 74-108	Exempts from mandatory public records disclosure
IL	75 Ill. Comp. Stat. Ann. 70/1	Disclosure prohibited
IN	Ind. Code Ann. § 5-14-3-4	Disclosure prohibited
IA	Iowa Code Ann. § 22.7	Disclosure prohibited
KS	Kan. Stat. Ann. § 45-221	Exempts from mandatory public records disclosure
KY	OAG 81-159 and OAG 82-149	Exempts from mandatory public records disclosure
LA	La. Stat. Ann. § 44:13	Disclosure prohibited
ME	Me. Rev. Stat. tit. 27, § 121	Disclosure prohibited
MD	Md. Educ. Code Ann. § 23-108	Disclosure prohibited
MD	MD GEN PROVIS § 4-308	Disclosure Prohibited
MA	Mass. Gen. Laws Ann. ch. 78, § 7	Exempts from mandatory public records disclosure
MI	Michigan Library Privacy Act; Mich. Comp. Laws Ann. § 397.603	Disclosure prohibited
MN	Minn. Stat. Ann. § 13.40	Disclosure prohibited
MS	Miss. Code. Ann. § 39-3-365	Disclosure prohibited
MO	Mo. Rev. Stat. Ann. § 182.817	Disclosure prohibited
MT	Montana Library Records Confidentiality Act; Mont. Code Ann. § 22-1-1103	Disclosure prohibited

NE	Neb. Rev. Stat. Ann. § 84-712.05	Exempts from mandatory public records disclosure
NV	Nev. Rev. Stat. Ann. § 239.013	Disclosure prohibited
NH	N.H. Rev. Stat. Ann. § 201-D:11	Disclosure prohibited
NH	N.H. Rev. Stat. Ann. § 91-A:5	Exempts from mandatory public records disclosure
NJ	N.J. Stat. Ann. § 18A:73-43.2	Disclosure prohibited
NM	Library Privacy Act; N.M. Stat. Ann. § 18-9-4	Disclosure prohibited
NY	N.Y. C.P.L.R. 4509	Disclosure prohibited
NC	N.C. Gen. Stat. Ann. § 125-19	Disclosure prohibited
ND	N.D. Cent. Code Ann. § 40-38-12	Disclosure prohibited
OH	Ohio Rev. Code Ann. § 149.432	Disclosure prohibited
OK	Okla. Stat. Ann. tit. 65, § 1-105	Disclosure prohibited
OR	Or. Rev. Stat. Ann. § 192.355	Disclosure prohibited
PA	24 Pa.C.S. § 9375	Disclosure prohibited
RI	11 R.I. Gen. Laws Ann. § 11-18-32	Disclosure prohibited
RI	38 R.I. Gen. Laws Ann. § 38-2-2	Exempts from mandatory public records disclosure
SC	S.C. Code Ann. § 60-4-10	Disclosure prohibited
SD	S.D. Codified Laws § 14-2-51	Disclosure prohibited
TN	Tenn. Code Ann. § 10-8-102	Disclosure prohibited
TX	Tex. Gov't Code Ann. § 552.124	Disclosure prohibited
UT	Utah Code Ann. § 63G-2-302	Disclosure prohibited
UT	Utah Code Ann. § 63G-2-201	Disclosure prohibited
UT	Utah Code Ann. § 63G-2-202	Disclosure prohibited
VT	Vt. Stat. Ann. tit. 22, § 172	Disclosure prohibited
VA	Va. Code Ann. § 2.2-3705.7	Exempts from mandatory public records disclosure
WA	Wash. Rev. Code Ann. § 42.56.310	Exempts from mandatory public records disclosure
WV	W. Va. Code Ann. § 29-1-8c	Disclosure prohibited
WI	Wis. Stat. Ann. § 43.30	Disclosure prohibited
WY	Wyo. Stat. Ann. § 16-4-203	Disclosure prohibited

Chart of Statutes Requiring a Court Order for Access to Library Records[1]

State	Statute	Type of Court Process Specified (if any)
AZ	Ariz. Rev. Stat. Ann. § 41-151.22	
AR	Ark. Code Ann. § 13-2-704	Warrant
AR	Ark. Code Ann. § 13-2-706	Warrant
CA	Cal. Gov't Code Ann. § 7927.105	
CO	Colo. Rev. Stat. Ann. § 24-90-119	Subpoena, warrant, or other legal requirement
CT	Conn. Gen. Stat. Ann. § 11-25	
DC	D.C. Code Ann. § 39-108	Subpoena
FL	Fla. Stat. Ann. § 257.261	
GA	Ga. Code Ann. § 24-12-30	Subpoena or court order
HI	Haw. Admin. R. § 8-200.5-3	Subpoena or court order
IL	75 Ill. Comp. Stat. Ann. 70/1	
IN	Ind. Code Ann. § 5-14-3-4	Court order in discovery, but silent on criminal proceedings
IA	Iowa Code Ann. § 22.7	
LA	La. Stat. Ann. § 44:13	
ME	Me. Rev. Stat. tit. 27, § 121	
MD	Md. Educ. Code Ann. § 23-108	Subpoena or court order
MI	Michigan Library Privacy Act; Mich. Comp. Laws Ann. § 397.603	
MN	Minn. Stat. Ann. § 13.40	
MS	Miss. Code. Ann. § 39-3-365	
MO	Mo. Rev. Stat. Ann. § 182.817	
MT	Montana Library Records Confidentiality Act; Mont. Code Ann. § 22-1-1103	
NV	Nev. Rev. Stat. Ann. § 239.013	
NH	N.H. Rev. Stat. Ann. § 201-D:11	Subpoena, court order or statutory requirement
NJ	N.J. Stat. Ann. § 18A:73-43.2	Subpoena issued by court or court order
NM	Library Privacy Act; N.M. Stat. Ann. § 18-9-4	
NY	N.Y. C.P.L.R. 4509	Subpoena, court order or statutory requirement
NC	N.C. Gen. Stat. Ann. § 125-19	Subpoena, court order or statutory requirement
ND	N.D. Cent. Code Ann. § 40-38-12	Subpoena or court order

[1] Empty cells indicate that the statute did not lay out a specific court process (i.e. a warrant or subpoena).

OK	Okla. Stat. Ann. tit. 65, § 1-105	
PA	24 Pa.C.S. § 9375	
SC	S.C. Code Ann. § 60-4-10	
SD	S.D. Codified Laws § 14-2-51	
TN	Tenn. Code Ann. § 10-8-102	
TX	Tex. Gov't Code Ann. § 552.124	Subpoena or court order
UT	Utah Code Ann. § 63G-2-202	
VT	Vt. Stat. Ann. tit. 22, § 172	Warrant or judicial order
WV	W. Va. Code Ann. § 29-1-8c	Subpoena or court order
WI	Wis. Stat. Ann. § 43.30 (West)	

Chart of Required Judicial Determinations or Safeguards for a Court Order Granting Access to Library Records to Issue

State	Statute	Requirement
Judicial Determinations		
IA	Iowa Code Ann. § 22.7	"The records shall be released only upon a judicial determination that a rational connection exists between the requested release of information and a legitimate end and that the need for the information is cogent and compelling."
MO	Mo. Rev. Stat. Ann. § 182.817	Allows disclosure "upon a finding that the disclosure of such record is necessary to protect the public safety or to prosecute a crime."
MT	Mont. Code Ann. § 22-1-1103	Allows disclosure in response to "an order issued by a court of competent jurisdiction, upon a finding that the disclosure of such record is necessary because the merits of public disclosure clearly exceed the demand for individual privacy"
NV	Nev. Rev. Stat. Ann. § 239.013	"Such records may be disclosed only in response to an order issued by a court upon a finding that the disclosure of such records is necessary to protect the public safety or to prosecute a crime."
SC	S.C. Code Ann. § 60-4-10	Allows disclosure "in accordance with proper judicial order upon a finding that the disclosure of the records is necessary to protect public safety, to prosecute a crime, or upon showing of good cause before the presiding Judge in a civil matter."
TX	Tex. Gov't Code Ann. § 552.124	Allows disclosure "to a law enforcement agency or a prosecutor under a court order or subpoena obtained after a showing to a district court that: (A) disclosure of the record is necessary to protect the public safety; or (B) the record is evidence of an

		offense or constitutes evidence that a particular person committed an offense."
Judicial Safeguards		
MI	Mich. Comp. Laws Ann. § 397.603	Allows for a library "to appear and be represented by counsel" in a court hearing on the requested disclosure.
NM	N.M. Stat. Ann. § 18-9-4	"The library shall have the right to be represented by counsel at any hearing on disclosure or release of its patron records."