Harvard Journal of Law & Technology
Volume 37, Number 1 Fall 2023

ILLUMINATING SURVEILLANCE: UPDATING RIGHTS OF ACCESS FOR ELECTRONIC SEARCHES

*Emily S. Shah**

ABSTRACT

Law enforcement has a growing array of electronic surveillance technologies at its disposal. From what we know, law enforcement use of these tools is extensive and invasive and has profoundly disparate impacts. But there is much we do not know.

The Supreme Court recently recognized the enormous privacy implications of electronic surveillance and its secrecy when it adopted a new approach to warrant requirements in *Carpenter*. While the Fourth Amendment and state statutes increasingly require law enforcement to obtain court authorization before an electronic search, those warrants remain almost universally sealed. As media and public interest organizations seek to unseal search warrants, right of access doctrines — rooted in the First Amendment and common law — have failed to adapt to the new state of surveillance.

This Note argues that the right of access doctrines, applied to electronic search warrants, should account for the implications of electronic surveillance, consistent with the Supreme Court's emerging perspective on electronic surveillance in the Fourth Amendment context. This Note explains how existing doctrines fail to account for the public's increased interests in electronic surveillance. And it proposes pathways for both courts and legislators to improve access to search warrants and begin improving accountability for electronic surveillance.

* Harvard Law School, Candidate for J.D., 2024; B.A.S., Stanford University, 2019. My sincerest thank you to Professor Susan Crawford, Professor Eisha Jain, Professor Laura Weinrib, Jacob Snow, and the editors of the *Harvard Journal of Law & Technology* for introducing me to the issues that inspired this paper, teaching me how to approach my first note, and sharing thoughtful and generous advice throughout the writing and editing process.

TABLE OF CONTENTS

I. INTRODUCTION 216

II. RIGHTS OF ACCESS TO SEARCH WARRANT MATERIALS 221
A. The Common Law Right of Access 223
1. Applications to Search Warrant Materials 224
B. The First Amendment Right of Access 227
1. Applications to Search Warrant Materials 229
a. Historical Openness 229
b. Positive Role in Functioning 231
c. Essential Closure and Narrow Tailoring 232

III. APPLYING RIGHTS OF ACCESS TO ELECTRONIC SEARCHES 233
A. Electronic Frontier Foundation v. Superior Court of San Bernardino County 234
1. First Amendment 236
2. Common Law 238
B. In re Leopold to Unseal Electronic Surveillance Applications and Orders 239
1. First Amendment 239
2. Common Law 240

IV. DISTINGUISHING ELECTRONIC WARRANTS 242

V. UPDATING THE RIGHTS OF ACCESS 246
A. Limits of Existing Doctrines 247
B. Updating the Rights of Access 249

VI. CONCLUSION 252

I. INTRODUCTION

Law enforcement agencies have a growing array of search technologies at their disposal. Immigration Customs and Enforcement ("ICE") Enforcement and Removal Operations officers have deployed Clearview AI's facial recognition software to investigate human trafficking.[1] Nebraska police charged a seventeen-year-old and her mother with felonies and misdemeanors after their Facebook messages, obtained with a court order, revealed they had purchased and used abortion

1. *See* Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/WE7H-BA88] (describing use of Clearview AI's facial recognition app in field offices and airports). ICE Homeland Security Investigations teams also use the technology to investigate cybercrimes, including child exploitation. *Id.*

medication.[2] Colorado police detained a Black family and handcuffed a twelve-year-old and a seventeen-year-old, after a system — possibly an automatic license plate reader ("ALPR") — misidentified their SUV's license plate as that of a stolen motorcycle.[3]

These technologies and others expand law enforcement's general power to monitor, investigate, and prosecute people.[4] That expanded power entrenches existing disparities in policing to disproportionately harm people of color, low-income communities, and other vulnerable populations. For instance, public housing residents are already subject to extensive video surveillance that law enforcement can leverage for historical or real-time facial recognition,[5] and facial recognition algorithms may be more likely to misidentify Black people.[6] Police disproportionately deploy ALPRs in low-income and non-White communities.[7] Geofence warrants, which require companies to provide

---

2. Jason Koebler & Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion*, MOTHERBOARD (Aug. 9, 2022), https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion--affidavit [https://perma.cc/RNM8-FL9X].

3. *See* Teo Armus, *Colorado Police Apologize Over Viral Video of Officers Handcuffing Black Girls in a Mistaken Stop*, WASH. POST. (Aug. 4, 2020), https://www.washingtonpost.com/nation/2020/08/04/aurora-pd-handcuffs-family-gunpoint/ [https://perma.cc/P4SV-MN2U]; Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CAL. L. REV. 917, 919–20 (2021) (describing use of ALPRs in incident); *see also* Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 505 (2019) (explaining that ALPRs can track cars' travel over a period of months or even years).

4. *See* Manes, *supra* note 3, at 506 ("Each of these technologies gives the police new and powerful capabilities to monitor people.").

5. *See* Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, WASH. POST (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/ [https://perma.cc/Z6T8-SERN] (describing punishment and evictions that result from extensive federally funded surveillance in public housing); *see generally* Lisa Lucile Owens, *Concentrated Surveillance Without Constitutional Privacy: Law, Inequality, and Public Housing*, 34 STAN. L. & POL'Y REV. 131, 171–77 (2023) (describing gaps in Fourth Amendment privacy doctrine for public housing–related information collection).

6. *See* GEO. L. CTR. ON PRIV. & TECH., THE PERPETUAL LINEUP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 53–54 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/PTH4-ZQSB] (describing study of three commercial algorithms finding 5–10% lower accuracy rates for African Americans compared to Caucasians, and similarly low accuracy rates for women compared to men); Kashmir Hill, *Your Face is Not Your Own*, N.Y. TIMES MAG., https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html [https://perma.cc/SNR8-KMDT] (describing 2019 National Institute of Standards and Technology study finding that "many algorithms were less accurate in identifying people of color" and noting three arrests of Black men based on incorrect facial recognition matching in 2020).

7. *See* Bloch-Wehba, *supra* note 3, at 919 (citing Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, ELEC. FRONTIER FOUND. (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data [https://perma.cc/67DK-YXJ6] (describing Oakland Police Department use of ALPRs to

law enforcement with a list of users in a specified location during a specified time frame, often identify suspects based on their presence in neighborhoods where crimes occur.[8]

Courts and legislatures have begun recognizing the extensive harms that these technologies can pose and a need for greater oversight. In the 2018 case *Carpenter v. United States*,[9] the Supreme Court described its concerns about the "deeply revealing nature" of collecting cell phone location information, the breadth of people it could affect, and the secrecy with which law enforcement could obtain it.[10] To facilitate greater accountability, *Carpenter* required law enforcement to obtain a warrant before collecting cell-site location information ("CSLI") over a four-month period.[11] Since 2016, the California Electronic Communications Privacy Act ("CalECPA") has also required governments in California to obtain a search warrant before accessing or compelling any electronic communications or metadata.[12] But the use of many modern surveillance technologies does not yet require warrants under the Constitution[13] or federal statutes.[14]

Search technologies are rapidly developing, and regulation of electronic surveillance is needed. Existing safeguards may not easily translate to new technologies, and diverse use cases may call for tailored

---

surveil Muslim communities during Ramadan and predominant use in Black and Latino neighborhoods in Oakland).

8. *See* Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021).

9. 138 S. Ct. 2206 (2018).

10. *Id.* at 2223; *see id.* at 2217–18 (explaining that digital location surveillance lacks the cost and labor limitations of physical surveillance); *see also* Hannah Bloch-Wehba, *Transparency After* Carpenter, 59 WASHBURN L.J. 23, 29 (2020) (describing *Carpenter* as expressing "unease about the secrecy and surreptitious nature of warrantless digital surveillance"); Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 6 (2020) (considering the "key" doctrinal takeaway from *Carpenter* to be the focus on the revealing nature, depth, breadth, reach, and "inescapable nature" of the data collection).

11. *Carpenter*, 138 S. Ct. at 2223. *But see id.* at 2212 (noting that the Stored Communications Act allows certain requests for information through a court order rather than a warrant).

12. CAL. PENAL CODE § 1546.1 (2016) (generally requiring warrant or similar prior authorization); *see also* UTAH CODE ANN. § 77-23-102 (2022) (requiring warrant for communications); VA. CODE ANN. § 19.2-70.3 (requiring warrant or similar prior authorization); ME. STAT. TIT. 16 § 648 (2019) (requiring warrant for GPS tracking).

13. *See* Bloch-Wehba, *supra* note 3, at 920–21 ("Modern policing depends on an array of techniques and technologies, like ALPRs, that are not considered 'searches and seizures' and therefore lie outside of the Fourth Amendment's protections."); *see also* Ben Vanston, *Putting Together the Pieces: The Mosaic Theory and Fourth Amendment Jurisprudence Since* Carpenter, 124 W. VA. L. REV. 657, 672–76 (2022) (describing narrow applications of *Carpenter* only to CSLI technology as of the publication of the article).

14. The 1986 Electronic Communications Privacy Act ("ECPA") governs surveillance of telephone and internet communications, *see* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 375 (2014), and only requires a warrant for real-time communications interception, *see* 18 U.S.C. § 2518, or unopened, stored communications less than 180 days old, *see* 18 U.S.C. § 2703(a).

protections.[15] And, given the significant privacy and liberty implications of these technologies, the people deserve a voice in this policymaking process.

Informed public participation requires that the public understand how governments are using surveillance technologies. Today, the technologies that agencies use, the frequency of use, the information they collect, and the way that judges review their requests are predominantly secret.[16] As a set of documents, electronic search warrants and their accompanying applications and affidavits could help answer these questions.[17]

Despite the status of government transparency as a democratic value, government officials tend to pay lip service to transparency while dragging their feet in practice.[18] Enacting policies to mandate reporting of electronic surveillance has taken years, if it succeeds at all.[19] Although a piecemeal and drawn-out approach, transparency litigation to unseal specific court records can force agencies to disclose their obscure investigative practices.[20] With that disclosure, the people can

---

15. For example, a warrant's particularity requirement might look different for searches of a non-physical space or the aggregation of various sources of public information. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 339 (2012); *see also* CAL. PENAL CODE § 1546.1(d)(1) (2016) (setting out new particularity requirements); Andrews v. Balt. City Police Dep't, 8 F.4th 234, 238 (4th Cir. 2020) (defining new particularity questions on remand to district court).

16. *See* Jonathan Manes, *supra* note 3, at 506–09; *see, e.g.*, LINDA LYE, ACLU OF N. CAL., STINGRAYS: THE MOST COMMON SURVEILLANCE TOOL THE GOVERNMENT WON'T TELL YOU ABOUT 9–10 (2014) (explaining difficulty of recognizing when cell-site simulators are used); *infra* notes 127–29 and accompanying text (discussing Electronic Frontier Foundation's specific request for information about quantity and context of cell-site simulator warrants); *infra* note 159 and accompanying text (describing request for sealed applications, orders, and docket numbers).

17. Law enforcement usually applies for a search warrant with an affidavit that alleges the facts that establish probable cause for a search of a person or place, the particular items they expect to find, and how that search will contribute to an investigation. *See* Wanda Ellen Wakefield, Annotation, *Disputation of Truth of Matters Stated in Affidavit in Support of Search Warrant — Modern Cases*, 24 A.L.R.4th 1266 § 2(a) (1983).

18. *See* Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 889–90, 898 (2006) (repeating argument that "the publicity of open government produces an informed and interested public," rather than "suspicious and/or ignorant masses"); Bloch-Wehba, *supra* note 3, at 926.

19. *See generally* Rachel Harmon, *Why Do We (Still) Lack Data on Policing?*, 96 MARQ. L. REV. 1119, 1128–32 (2013) (describing local government officials' incentive structures that induce less information collection and reporting than the public demands). In 2017, New York City Council proposed the Public Oversight of Surveillance Technology Act, which required annual reporting on every surveillance technology the NYPD uses. Bloch-Wehba, *supra* note 3, at 955. The proposal stalled for three years before it was passed in June 2020, at which point, the NYPD still refused to release certain predictive policing records because of the provider, Palantir's, trade secrets. *Id.* at 955–56. And in states with automatic unsealing laws that require search warrants to be made public after a specified period of time, courts have stepped in to carve out exceptions. *See, e.g.*, CAL. PENAL CODE § 1534(a) (2021); Elec. Frontier Found. v. Super. Ct. of San Bernardino Cnty., 299 Cal. Rptr. 3d 480 (Ct. App. 2022).

20. Bloch-Wehba, *supra* note 3, at 922.

understand surveillance practices and existing policy gaps, and they can organize for meaningful change.[21]

Although the public has a right of access to judicial records, organizations seeking to unseal search warrants — even long after their execution — often fail.[22] For more than thirty years, scholars have criticized right of access doctrines for their inconsistency and their failure to realize court transparency and government accountability.[23] Other scholars criticize Fourth Amendment doctrine for drifting too far from its roots in protecting the public from government searches.[24] And recent scholarship has detailed the harms that electronic surveillance

21. *Id.* A successful example is Freedom of Information Law litigation in New York City, which publicized the NYPD's documentation of Stop and Frisk, exposing the sheer quantity of stops, the frequency with which stops led to police using force against a person, the rarity of occasions in which a frisk led to an actual arrest, and the enormous racial disparities and disproportionate effects on Black and Latino people. *See id.* at 944–47 (citing Verified Petition, N.Y. Civil Liberties Union v. NYPD, 866 N.Y.S.2d 93 (Super. Ct. 2008) (No. 115154/07), 2007 WL 3390434); *see also Stop-and-Frisk Data*, NYCLU, https://www.nyclu.org/en/stop-and-frisk-data [https://perma.cc/7R9H-L8W7] (linking transparency and public participation to debates about making police more accountable or democratic).

22. Courts usually issue search warrants under seal to avoid allowing the people targeted to conceal or destroy evidence, but as searches are executed, indictments are brought, and defendants are convicted, the reasons for maintaining secrecy weaken. *See* Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Search Orders*, 93 WASH. L. REV. 145, 194–95 (2018); *In re* Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008) ("Such restrictions on speech and public access are presumptively justified while the investigation is ongoing, but that justification has an expiration date.").

23. *See, e.g.*, Shira Poliak, Comment, *The Logic of Experience: The Role of History in Recognizing Public Rights of Access Under the First Amendment*, 167 U. PA. L. REV. 1561, 1564 (2019) (citing David Ardia, *Court Transparency and the First Amendment*, 38 CARDOZO L. REV. 835, 840 (2017); Raleigh Hannah Levine, *Toward a New Public Access Doctrine*, 27 CARDOZO L. REV. 1739, 1758–76 (2006)); Bloch-Wehba, *supra* note 22, at 193–95; Michael J. Hayes, Note, *What Ever Happened to the "Right to Know"?: Access to Government-Controlled Information Since* Richmond Newspapers, 73 VA. L. REV. 1111, 1131–32 (1987); Kimba M. Wood, *Re-Examining the Access Doctrine*, 11 COMM. LAW. 3, 3–5 (1994); Judith Resnik, *The Contingency of Openness in Courts: Changing the Experiences and Logics of the Public's Role in Court-Based ADR*, 15 NEV. L.J. 1631, 1670–71 (2015).

24. *See, e.g.*, Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303 (2010) (making textual and historical arguments for reading Fourth Amendment as political protections); David Gray, *Collective Standing Under the Fourth Amendment*, 56 AM. CRIM. L. REV. 77 (2018) (arguing for a security-based conception of Fourth Amendment); Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1 (2013) (arguing Fourth Amendment balancing tests forget that criminal defendants' rights matter to larger society); David Gray, *A Collective Right to be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189 (2015) (arguing for technology-centered approach to regulation); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 118–19 (2008) (arguing for politicizing the Fourth Amendment by interpretating it as negotiation between people and their government about boundaries of law enforcement power).

technologies pose and identified opportunities for legal and policy responses.[25]

This Note synthesizes these criticisms to evaluate how the Fourth Amendment's recent attention to the public's interests in electronic surveillance might strengthen right of access doctrines. For decades, courts have diverged on whether and how rights of access apply to search warrants.[26] Considering whether to require a search warrant, the Supreme Court recently acknowledged that electronic surveillance enables deeper and broader privacy invasions, allows for increased law enforcement secrecy, and necessitates a policy response.[27] This Note argues that the Court's recognition of greater public interests in understanding electronic surveillance should influence the public right of access to electronic search warrant materials.[28]

This Note proceeds as follows. Part II provides a background on right of access doctrines, rooted in the common law and First Amendment, and explores the inconsistent ways courts have applied those doctrines to search warrants. Part III describes two recent cases to illustrate how those doctrines have struggled to realize transparency in unsealing modern electronic search warrant materials. Part IV discusses how recent Supreme Court opinions distinguished electronic surveillance from traditional surveillance in considering whether the Fourth Amendment requires a warrant. Part V explores how the reasoning in those opinions can enable a meaningful right of access to electronic warrant materials by arguing within existing doctrines or by updating them. Part VI concludes.

II. RIGHTS OF ACCESS TO SEARCH WARRANT MATERIALS

The Supreme Court has recognized rights of access to court records deriving from the common law and from the First Amendment.[29] These doctrines create the potential for expansive judicial transparency,[30] but

25. *See, e.g.*, Manes, *supra* note 3, at 557–66 (proposing reforms for electronic surveillance's secrecy); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1112–26 (2016) (developing administrative framework to regulate programmatic surveillance); Kerr, *supra* note 14, at 411–18 (describing amendments to 1986 Electronic Communications Privacy Act to respond to modern surveillance).

26. *See infra* Sections II.A.1, II.B.1.

27. *See infra* Part IV.

28. *See infra* Section V.B.

29. Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978) (acknowledging common law right to access court records); Press-Enter. Co. v. Super. Ct. of Cal. for Riverside Cnty. (*Press-Enterprise II*), 478 U.S. 1, 13 (1986) (extending First Amendment right to access preliminary hearings).

30. This Note focuses on rights of access to court records. Statutorily created rights of access to other public records, *see, e.g.*, Freedom of Information Act, 5 U.S.C. § 552, are beyond the scope of this analysis. Moreover, a number of these statutory rights do not apply

in applying them to search warrants, federal circuit courts have not only taken inconsistent approaches but also generally limited the rights.[31] The common law right presumes the public has interests in access to court records, but reviewing courts grant significant discretion to sealing judges to weigh them.[32] And, while the First Amendment right constrains judges' discretion, many courts have considered search warrant materials beyond the scope of the First Amendment right.[33]

There can be important reasons to seal search warrants and their application materials. The government often opposes unsealing on the grounds that it would harm ongoing investigations.[34] By revealing the "nature, scope[,] and direction of the government's investigation," the unsealed materials could allow targets to alter evidence or otherwise hinder the investigation.[35] They could also risk exposing confidential informants, who would hesitate to contribute to warrant affidavits.[36] Although the government most often opposes unsealing, publicized search warrant materials can also harm defendants and others. Warrant affidavits might include information that sways potential juries and infringes on defendants' fair trial rights.[37] The warrant materials might

---

to records of court proceedings. *See id.* ("Each *agency* shall make available to the public information as follows . . .") (emphasis added); Jennifer Jansutis, *FOIA 101: Demystifying Public Records Laws in Each State*, GRANICUS, https://granicus.com/blog/foia-101-public-record-laws-in-each-state/ [https://perma.cc/H5SD-CVCA] (noting public records laws do not apply to non-administrative court records in at least D.C., Massachusetts, Maine, Michigan, Minnesota, Mississippi, New York, Rhode Island, and Virginia).

31. *See infra* Sections II.A.1, II.B.1. This Note focuses on warrants required by the Fourth Amendment, but there are also statutes like the 1986 Electronic Communications Privacy Act, that mandate warrants or other court authorization procedures for electronic surveillance. *See* 18 U.S.C. §§ 2518, 2703, 3117, 3122, 3123.

32. *See infra* Section II.A.1.

33. *See infra* Section II.B.1.

34. *See, e.g.*, Times Mirror Co. v. United States, 873 F.3d 1210, 1215 (9th Cir. 1989) (describing concerns about disclosure during ongoing investigation); *In re* EyeCare Physicians of Am., 100 F.3d 514, 519 (7th Cir. 1996) ("[D]isclosure of the affidavits might very likely impair the ongoing criminal investigation.").

35. *In re* Search Warrant for Secretarial Area Outside Off. of Gunn, 855 F.2d 569, 574 (8th Cir. 1988); *see In re EyeCare Physicians*, 100 F.3d at 519 ("[D]isclosing even a redacted version of the search warrant affidavit would enable the subjects of the investigation the opportunity to alter, remove or withhold records.").

36. *See, e.g.*, *In re EyeCare Physicians*, 100 F.3d at 518 n.5 (describing informant's privilege as reason to avoid disclosure); Lawmaster v. United States (*In re* Search of 1638 E. 2nd St., Tulsa, Okla.), 993 F.2d 773, 774 (10th Cir. 1993) (relying on need to protect confidential informant); *see also* United States v. Sealed Search Warrants, 868 F.3d 385, 395 (5th Cir. 2017) ("[U]nsealing . . . might endanger or discourage witnesses from providing evidence or testimony.").

37. *See* Gardner v. Newsday, Inc. (*In re* Application of Newsday, Inc.), 895 F.2d 74, 79 (2d Cir. 1990) (considering "privacy rights of . . . parties to the intercepted communications"). This interest is less often raised by the government when opposing unsealing, but criminal defendants have raised it. *See* Wash. Post Co. v. Hughes (*In re* Application & Affidavit for a Search Warrant), 923 F.2d 324, 328–29 (4th Cir. 1991) (rejecting defendant's claim that the district court abused its discretion by releasing a search warrant affidavit after finding "asserted rights are [not] actually compromised" given voir dire); *see also id.* at 330–31 (finding

also harm the reputations of targets or others mentioned within them by tying them to a criminal investigation, even if there is insufficient evidence any indictment will follow.[38] As the following Sections explain, courts weigh these interests as they apply the common law and First Amendment rights of access to search warrant materials.

A. The Common Law Right of Access

The common law right of access emerged from a longstanding assumption that the judiciary has no more of a right than "other institutions of democratic government[] to suppress, edit, or censor events which transpire in proceedings before it."[39] The common law right extends to judicial records in criminal and civil proceedings.[40]

In *Nixon v. Warner Communications, Inc.*,[41] the Supreme Court articulated a balancing test for the "general right to inspect and copy . . . judicial records and documents."[42] Addressing broadcasters' requests for the tapes played in the Watergate trials, the *Nixon* Court began with the presumption that the public has legitimate interests in "keep[ing] a watchful eye on the workings of public agencies" and "publish[ing] information concerning the operation of government."[43] But interests in secrecy could outweigh the presumed interests if a court found so "in light of the public interest and the duty of the courts."[44] The Court gave considerable deference to the "sound discretion of the trial court . . . in light of the relevant facts and circumstances of the particular case."[45]

---

that, in the context of the criminal justice system, public interest in right of access "may be magnified" given importance of understanding "patterns of crime" and how well law enforcement systems work).

38. *See Sealed Search Warrants*, 868 F.3d at 395 ("[T]he publication of a warrant could damage an unindicted target's reputation while leaving no judicial forum to rehabilitate that reputation."); United States v. Bus. of Custer Battlefield Museum & Store Located at Interstate 90, Exit 514, S. of Billings, Mont., 658 F.3d 1188, 1191 (9th Cir. 2011) (raising similar concerns); *In re EyeCare Physicians*, 100 F.3d at 519 (same).

39. Craig v. Harney, 331 U.S. 367, 374 (1947) (explaining why "[w]hat transpires in the court room is public property"); *see also* Hicklin Eng'g, L.C. v. Bartell, 439 F.3d 346, 348 (7th Cir. 2006) ("Judges deliberate in private but issue public decisions after public arguments based on public records. . . . Any step that withdraws an element of the judicial process from public view makes the ensuing decision look more like fiat and requires rigorous justification.").

40. *See* Perez-Guerrero v. U.S. Att'y. Gen., 717 F.3d 1224, 1235 (11th Cir. 2013) ("[Courts] 'traditionally distinguish between those items which may properly be considered public or judicial records and those that may not; the media and public presumptively have access to the former, but not to the latter.'" (quoting Chi. Trib. Co. v. Bridgestone/Firestone, Inc., 263 F.3d 1304, 1311 (11th Cir. 2001))). Nonjudicial records include private parties' documents; an example of nonjudicial records in the civil context is discovery materials. *See Chi. Trib.*, 263 F.3d at 1311.

41. 435 U.S. 589 (1978).

42. *Id.* at 597.

43. *Id.* at 597–98.

44. *Id.* at 602.

45. *Id.* at 599.

Because the lower court relied on factors that were no longer relevant,[46] the Supreme Court found that the public's interests in the tapes significantly outweighed President Nixon's stated property and privacy interests.[47] Ultimately, however, the Court declined to order the release of the recordings as it would frustrate a separate administrative procedure for such releases.[48]

As articulated in *Nixon*, the common law right of access begins with a powerful presumption of legitimate public interests in and access to all judicial records.[49] But because *Nixon* requires a court to evaluate, in each particular case, whether secrecy interests outweigh the public's interests, the common law right leaves significant discretion to the sealing officer. This discretion makes it more difficult to successfully reverse a trial court's decision, and it may allow courts to keep documents secret with limited explanation, which limits public understanding even further. As the following Section explains, circuit courts require trial courts to provide varying levels of explanation when they refuse to unseal search warrant materials.

1. Applications to Search Warrant Materials

The common law right of access presents a promising pathway to access search warrant materials, in part because courts must consider the secrecy interests in the particular documents requested, rather than overarching government concerns about access. Circuit courts generally agree that search warrants are judicial records within the scope of the common law right of access[50] and review a sealing judge's decision

46. *Id.* at 602 n.14 (explaining that the lower court refused access because defendants were still appealing convictions, but by the time of the Supreme Court's review, appeals had been resolved).

47. *Id.* at 600–02.

48. *Id.* at 603–06 (explaining access might frustrate Presidential Recording Act's goal of "orderly processing"). A statute can supersede the common law right. *See, e.g.*, *In re* N.Y. Times Co. to Unseal Wiretap & Search Warrant Materials, 577 F.3d 401, 404–05, 408 (2d Cir. 2009) (finding Wiretap Act created procedure that superseded the common law right by requiring "showing of good cause" by the target of the search to unseal a Wiretap Act warrant).

49. Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597–98 (1978); *see* Lynn B. Oberlander, *A First Amendment Right of Access to Affidavits in Support of Search Warrants*, 90 COLUM. L. REV. 2216, 2217 (1990).

50. *See, e.g.*, *In re* L.A. Times Commc'ns LLC, 28 F.4th 292, 297 (D.C. Cir. 2022) (explaining search warrant materials "would have been intended to influence a judicial decision to find probable cause to issue a search warrant"); Balt. Sun Co. v. Goetz, 886 F.2d 60, 63–64 (4th Cir. 1989) (considering affidavits for search warrants to be judicial records because Federal Rule of Criminal Procedure 41(g) requires filing with court clerk); United States v. Bus. of Custer Battlefield Museum & Store Located at Interstate 90, Exit 514, S. of Billings, Mont., 658 F.3d 1188, 1193 (9th Cir. 2011) (finding post-investigation warrant materials subject to public right of access); Gardner v. Newsday, Inc. (*In re* Application of Newsday, Inc.), 895 F.2d 74, 79 (2d Cir. 1990) (same); Lawmaster v. United States (*In re* Search of 1638 E. 2nd St., Tulsa, Okla.), 993 F.2d 773, 775 (10th Cir. 1993) (same).

under an abuse of discretion standard.[51] But the intensity of appellate review varies significantly with respect to the factors sealing judges must consider and the explanation they must provide. Adding structure to a judge's decision to seal or unseal documents might not always translate to a stronger right of access, but it does create some accountability for judges to honor that right.

In the D.C. Circuit, judges sealing search warrant materials must consider six factors to evaluate whether secrecy interests outweigh the presumption of public access.[52] Since 1980, these six factors have included:

> (1) the need for public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure, and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings.[53]

In the 2022 case *In re Los Angeles Times Communications LLC*, the *Los Angeles Times* sought to unseal search warrant materials related to an investigation into a United States senator's potential insider trading.[54] The D.C. Circuit held that the district court failed to consider the public's interests in a sitting senator's potential illegal activity, the senator's public acknowledgment of the investigation, the fact that his actions were taken in an official capacity, and how the warrant materials affected the judge's decision.[55] Remanding, the D.C. Circuit required the sealing judge to analyze each factor with a "'full explanation' . . . to enable this court['s] review."[56]

The Fourth Circuit's test has fewer requirements: the sealing judge must articulate the interest that sealing protects, supported by "findings

---

51. *See, e.g.*, *Balt. Sun Co.*, 886 F.2d at 64; United States v. Sealed Search Warrants, 868 F.3d 385, 396 (5th Cir. 2017); *Bus. of the Custer Battlefield Museum & Store*, 658 F.3d at 1195; *In re* Search of Fair Fin., 692 F.3d 424, 431 (6th Cir. 2012); *In re* EyeCare Physicians of Am., 100 F.3d 514, 518 (7th Cir. 1996); *In re 1638 E. 2nd St.*, 993 F.2d at 774; *In re L.A. Times*, 28 F.4th at 297.

52. *In re L.A. Times*, 28 F.4th at 297 (citing United States v. Hubbard, 650 F.2d 293, 317–22 (D.C. Cir. 1980)).

53. *Id.* (citing MetLife v. Financial Stability Oversight Council, 865 F.3d 661, 665 (D.C. Cir. 2017)); *see also In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold III*), 964 F.3d 1121, 1131 (D.C. Cir. 2020) (applying test).

54. *In re L.A. Times*, 28 F.4th at 295.

55. *Id.* at 298.

56. *Id.* at 298–99 (quoting EEOC v. Nat'l Children's Ctr., Inc., 98 F.3d 1406, 1410 (D.C. Cir. 1996)).

specific enough" to enable appellate review.[57] The sealing judge "may explicitly adopt the facts that the government presents" and file "the government's submission and the officer's reason[ing]" under seal.[58] But in 1989, the Fourth Circuit vacated a district court sealing order because the judge failed to consider alternatives to sealing a warrant affidavit.[59] By requiring consideration of alternatives, including redaction, the Fourth Circuit might heighten the standards for refusing unsealing.

The Fifth and Sixth Circuits also require the sealing judge's explanation to include sufficient findings on the harms that public access would pose.[60] In 2017, the Fifth Circuit considered insufficient a sealing judge's conclusory statement that "there is a substantial probability that the investigation will be compromised if the affidavit is unsealed."[61] Applying a similar standard, the Sixth Circuit affirmed the sealing judge's adoption of the government's explanation of why disclosure would harm its investigation.[62] At least in the Sixth Circuit, however, the "articulation requirement exists only to aid reviewing courts rather than for the benefit of the public."[63]

The Ninth, Tenth, and possibly the Seventh Circuits have shifted further from *Nixon*'s case-by-case review and presumption of access. The Ninth Circuit does not recognize a common law right of access to warrant materials before indictment.[64] In *Times Mirror Co. v. United States*,[65] media organizations sought warrant materials for an FBI investigation into military procurement corruption.[66] After stating a requirement that parties seeking access must meet an "important public

57. Balt. Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989) (quoting Press-Enter. Co. v. Super. Ct. of Cal. (*Press-Enterprise I*), 464 U.S. 501, 510 (1984)). The *Baltimore Sun* sought to unseal warrant affidavits before indictment for an FBI investigation into healthcare industry fraud. 886 F.2d at 62–63.

58. 886 F.2d at 65.

59. *Id.* at 66. It is worth noting that in this common law right of access analysis, the Fourth Circuit relied on a line of cases interpreting the First Amendment right of access. *Id.* at 64. This case might also be unusual because the district court rejected the government's own offer to release a redacted version of the affidavit. *See id.* at 63, 66.

60. *See* United States v. Sealed Search Warrants, 868 F.3d 385, 397 (5th Cir. 2017) (requiring court to, on a case-by-case basis, "articulate any reasons that would support sealing [a judicial document]" or "'explain why it chose to seal [a judicial document]' . . . with a level of detail that [would] allow for this Court's review") (quoting SEC v. Van Waeyenberghe, 990 F.2d 845, 849 (5th Cir. 1993) and United States v. Holy Land Found. for Relief & Dev., 624 F.3d 685, 690 (5th Cir. 2010)); *In re* Search of Fair Fin., 692 F.3d 424, 433–34 (6th Cir. 2012) ("[R]eversal on this basis is appropriate only where a sealing court's deficient articulation of its decision impedes review.").

61. *Sealed Search Warrants*, 868 F.3d at 397; *see id.* at 390 (considering taxpayer seeking warrant affidavits for search of his home after warrant's execution).

62. *In re Fair Fin.*, 692 F.3d at 427, 434.

63. *Id.* at 434.

64. Times Mirror Co. v. United States, 873 F.2d 1210, 1219–20 (9th Cir. 1989).

65. 873 F.2d 1210 (9th Cir. 1989).

66. *Id.* at 1211.

need or 'ends of justice' standard,"[67] the court concluded that the "ends of justice" would never be served "if the public were allowed access to warrant materials in the midst of a preindictment investigation into suspected criminal activity."[68] The Tenth Circuit denies the presumption of public access to warrant materials "properly submitted under seal."[69] In *Lawmaster v. United States* (*In re Search of 1638 E. 2nd St., Tulsa, Oklahoma*),[70] the subject of a "fruitless" search of his home sought to unseal the warrant affidavit.[71] The court held that the presumption alone could not overcome the properly invoked informer's privilege, which protects the state from disclosing an informant's identity.[72] The Seventh Circuit has indicated it would take a similar approach.[73]

Given the sealing judge's discretion and the requirement of case-by-case review, the common law right of access might vary significantly in its outcomes. But circuit courts also lay out various standards for reviewing the sealing judge's approach, ranging from requiring multifactor tests, to focusing on the supporting evidence, to drawing bright-line rules. The extent and type of explanation that judges provide when they choose to seal search warrant materials determines how well the public can understand why and impose accountability.

B. The First Amendment Right of Access

Unlike the common law right, the First Amendment right of access requires a judge to provide specific findings that closure is narrowly tailored to meet an essential need. But a judge must first determine whether the First Amendment right even applies to a category of documents. Given its narrower scope, litigants have struggled to argue that the First Amendment right of access should apply to search warrant materials.

---

67. *Id.* at 1219.

68. *Id.*; *see also* United States Dep't of Just. v. ACLU, 812 F. App'x 722, 724 (9th Cir. 2020) (holding government interest in secrecy in ongoing investigation outweighs any presumption of access); United States v. Bus. of Custer Battlefield Museum & Store Located at Interstate 90, Exit 514, S. of Billings, Mont., 658 F.3d 1188, 1195 (9th Cir. 2011) (allowing common law balancing post-indictment).

69. Lawmaster v. United States (*In re* Search of 1638 E. 2nd St., Tulsa, Okla.), 993 F.2d 773, 775 (10th Cir. 1993) (quoting United States v. Corbitt, 879 F.2d 224, 228 (7th Cir. 1989)).

70. 993 F.2d 773 (10th Cir. 1993).

71. *Id.* at 774.

72. *Id.* at 775 (citing *Times Mirror Co.*, 873 F.2d at 1219 ("[T]here is no right of access to documents which have traditionally been kept secret for important policy reasons.")); *see also id.* at 774 (citing Hoffman v. Reali, 973 F.2d 980, 987 (1st Cir.1992); Dole v. Local 1942, 870 F.2d 368, 372 (7th Cir.1989)) (describing informer's privilege as protection of informants from reprisal).

73. *Corbitt*, 879 F.2d at 228 (refusing access to sealed presentence report after holding that "[w]here judicial records are confidential, the party seeking disclosure may not rely on presumptions but must instead make a specific showing of need for access to the document").

In 1986, in *Press-Enterprise Company v. Superior Court of California* (*Press-Enterprise II*),[74] the Supreme Court articulated a First Amendment right of access to judicial proceedings.[75] In 1981, California charged Robert Diaz with twelve counts of murder.[76] Diaz asked the trial court to seal the preliminary hearing transcripts, and when *Press-Enterprise*, a local news organization, sought access, the magistrate judge refused.[77] The California Supreme Court held that Supreme Court precedent only recognized access to criminal proceedings in actual trials, where there was less concern that future jury members would be swayed by the newspaper's coverage.[78]

Press-Enterprise appealed to the Supreme Court, which held that a qualified First Amendment right of access attaches to a particular proceeding if (1) "the place and process have historically been open to the press and general public," and (2) "public access plays a significant positive role in the functioning of the particular process in question."[79] If the First Amendment right attaches, a party seeking to seal a proceeding must provide evidence that in that specific case, "closure is essential to preserve higher values and is narrowly tailored to serve that interest."[80]

The Supreme Court found that the First Amendment right attached to California's preliminary hearings because they had traditionally been open to the public[81] and because observation of them provided a safeguard to defendants and strengthened public confidence in the criminal justice system.[82] The Court then reversed the California Supreme Court's decision because it required only a "reasonable likelihood" of prejudice to the defendant's rights and failed to consider alternatives short of complete closure to protect the defendant's interests.[83]

If the First Amendment right attaches to a category of proceedings or documents, those seeking to prevent access face a higher burden of proof. But litigants have struggled to demonstrate that history and

74. 478 U.S. 1 (1986).

75. *Id.* at 10–13. *Press-Enterprise II* developed from earlier cases recognizing a public right of access specifically to criminal trials. *Id.* at 8–10; *see also* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980) (closed murder trial); Globe Newspaper Co. v. Super. Ct. for Norfolk Cnty., 457 U.S. 596 (1982) (juvenile victims of sexual assault testifying at trials); Press-Enter. Co. v. Super. Ct. of Cal. (*Press-Enterprise I*), 464 U.S. 501 (1984) (voir dire).

76. *Press-Enterprise II*, 478 U.S. at 3.

77. *Id.* at 3–5.

78. *Id.* at 5.

79. *Id.* at 8.

80. *Id.* at 9 (citing *Press-Enterprise I*, 464 U.S. at 510).

81. *Id.* at 10–11 (describing Aaron Burr's open preliminary hearing in 1807 and consistent state and federal practices since).

82. *Id.* at 12–13 (considering access to preliminary hearing transcript a safeguard for defendants in proceedings without a jury and an opportunity to build public confidence in functioning of criminal justice system).

83. *Id.* at 14–15.

functioning support attaching the First Amendment right to search warrant materials as a category of documents.

1. Applications to Search Warrant Materials

Public right of access claims multiplied in the years following *Press-Enterprise II*, and circuit courts quickly split on whether the First Amendment right of access attached to search warrant materials.[84] The circuits' inconsistent approaches to the history and functioning prongs in the search warrant context have led some scholars — in the 1990s and more recently — to criticize the First Amendment right of access test.[85]

a. Historical Openness

The *Press-Enterprise II* test first asks whether "the place and process have historically been open to the press and general public."[86] Although *Press-Enterprise II* considered judicial proceedings, several circuit courts have assumed that the First Amendment right of access also applies to judicial documents.[87] But their methodologies differ: some circuits simply ask whether history supports access to the documents, and others consider access to documents a necessary corollary of access to the relevant proceeding.[88]

Several circuits have taken the first approach and conditioned access to search warrant materials on access to warrant proceedings.[89] In 1989, while evaluating requests to unseal search warrant materials for an investigation into defense procurement corruption, the Ninth Circuit considered the applicable tradition to be the search warrant proceedings, which are conducted after a government's ex parte application and

84. *See* Poliak, *supra* note 23, at 1573–74; *see, e.g.*, Dhiab v. Trump, 852 F.3d 1087, 1107 (D.C. Cir. 2017) (Williams, J., concurring) ("[W]e have little guidance from the Supreme Court, or indeed any other, as to how to make [the relevant] choices."). This Section only discusses circuit courts, though district courts and state courts are also grappling with this question.

85. *See, e.g.*, Poliak, *supra* note 23, at 1564; Hayes, *supra* note 23, at 1131–32; Wood, *supra* note 23, at 3–5; Jeffrey L. Levy, *An Ill Wind Blows: Restricting the Public's Right of Access to Search Warrant Affidavits*, 74 MINN. L. REV. 661, 678 (1990).

86. *Press-Enterprise II*, 478 U.S. at 8.

87. Several circuit courts have extended *Press-Enterprise II*'s test to judicial documents. *See* Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 91–92 (2d Cir. 2004) (collecting cases). The Supreme Court has not clarified whether the First Amendment right of access applies to judicial documents in the same way as proceedings. *See id.* at 91; Levy, *supra* note 85, at 678.

88. *Hartford Courant Co.*, 380 F.3d at 91–92; *see* Levy, *supra* note 85, at 678.

89. *See, e.g.*, Times Mirror Co. v. United States, 873 F.2d 1210, 1211 (9th Cir. 1989); *In re* Search of Fair Fin., 692 F.3d 424, 433 (6th Cir. 2012); Balt. Sun Co. v. Goetz, 886 F.2d 60, 64–65 (4th Cir. 1989).

a judge's in camera consideration.[90] Because the associated proceedings were historically closed, the Ninth Circuit held that there was no First Amendment right of access to search warrant materials, at least before indictment.[91] The year before, while considering warrant materials related to the same FBI investigation, the Eighth Circuit held that the long tradition of filing unsealed search warrant materials with court clerks after their execution provided a historical tradition of the documents' openness.[92] Although the Eighth Circuit's approach strengthens arguments for a First Amendment right of access to search warrant materials, the Supreme Court has not clarified which approach to *Press-Enterprise II*'s history prong is correct.[93]

More broadly, scholars have criticized the "history" prong for the inconsistent approaches and interpretations it has generated.[94] Other scholars have argued the historical openness prong is out of touch with changing judicial practices: in particular, the fact that modern criminal proceedings are increasingly settled in plea bargain proceedings rather than public trials.[95] And recently, scholars have raised concerns about First Amendment doctrine's growing reliance on historical tradition, given its contested historical scope and the twentieth-century origins of many of its protections.[96]

---

90. *Times Mirror Co.*, 873 F.2d at 1214 (noting government has always been allowed to request a sealing order to avoid publicly filing search warrant documents and rejecting approach in *In re* Search Warrant for Secretarial Area Outside Off. of Gunn, 855 F.2d 569, 573 (8th Cir. 1988)).

91. *Id.* at 1214; *see also* U.S. Dep't of Just. v. ACLU, 812 F. App'x 722, 723 (9th Cir. 2020) (interpreting *Times Mirror Co.* to bar access during ongoing investigation); *Balt. Sun Co.*, 886 F.2d at 64–65 (also considering public access to search warrant proceedings).

92. *In re Gunn*, 855 F.2d at 573; *see also* Oberlander, *supra* note 49, at 2223.

93. See Levy, *supra* note 85, at 678; Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 92–93 (2d Cir. 2004); *see also* Bloch-Wehba, *supra* note 22, at 183–84 (arguing most analogous process is not the search warrant proceeding or filing, but the search itself, which was public from the Founding Era until the early twentieth century).

94. *See* Poliak, *supra* note 23, at 1564–65 (citing David Ardia, *Court Transparency and the First Amendment*, 38 CARDOZO L. REV. 835, 840 (2017) and Raleigh Hannah Levine, *Toward a New Public Access Doctrine*, 27 CARDOZO L. REV. 1739, 1758–76 (2006)); *see generally* Poliak, *supra* note 23, at 1573–89 (categorizing right of access cases by types of "history" scholars used).

95. *See, e.g.*, Wood, *supra* note 23, at 3–5; Resnik, *supra* note 23, at 1670–71.

96. Since *Press-Enterprise II*, the Supreme Court has expanded its reliance on historical tradition in First Amendment cases. *Compare* Hayes, *supra* note 23, at 1131–32 (in 1987, criticizing experience prong as inconsistent with other First Amendment doctrines), *with* Marc O. DeGirolami, *First Amendment Traditionalism*, 97 WASH. U. L. REV. 1653, 1657–58 (2020) (citing recent cases using tradition to determine unprotected categories of speech, government speech, political speech, and Establishment Clause). But debates about the original meaning of the First Amendment and the twentieth-century expansion of the First Amendment's protections make concerns about historical approaches to broader constitutional law especially poignant. *See* Caroline Mala Corbin, *Free Speech Originalism: Unconstraining in Theory and Opportunistic in Practice*, 92 GEO. WASH. L. REV. (forthcoming 2023) (manuscript at 18–19), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466315 [https://perma.cc/EWH4-6BRR]; Emily Erickson & Matthew D. Bunker, *The Jurisprudence of Tradition:*

b. Positive Role in Functioning

The second prong of the *Press-Enterprise II* test asks "whether public access plays a significant positive role in the functioning of the particular process in question."[97] Applying the functioning prong to search warrants, circuit courts disagree on whether to consider only the positive role that public access would play or to weigh those benefits against potential harms of disclosure.[98] Courts further debate what benefits and harms matter.

The Eighth Circuit focuses only on the positive role that public access could play, while the Ninth Circuit weighs similar benefits against the harms that public access could pose. In cases involving nearly identical facts, those differing approaches drove the courts to opposing conclusions.[99] The Eighth Circuit found that access to search warrants "is important to the public's understanding of the functioning and operation of the judicial process and the criminal justice system and may operate as a curb on prosecutorial or judicial misconduct."[100] On the other hand, the Ninth Circuit concluded that "public access would hinder, rather than facilitate, the warrant process and the government's ability to conduct criminal investigations."[101]

Courts also disagree about what benefits and harms are relevant to the functioning prong. Unlike the Eighth Circuit, which focuses on the public's interests,[102] the Sixth Circuit considers only the incremental benefit that public access would provide potential defendants.[103] Although *Press-Enterprise II* specifies a focus on "the particular process

Constitutional Gaslighting and the Future of First Amendment Free Speech Doctrine, 29 WIDENER L. REV. 139, 164–67 (2023); *see also* Jack M. Balkin, *The New Originalism and the Uses of History*, 82 FORDHAM L. REV. 641, 678 (2013) (raising interpretive concerns about conflicting histories).

97. Press-Enter. Co. v. Super. Ct. of Cal. for Riverside Cnty. (*Press-Enterprise II*), 478 U.S. 1, 8 (1986).

98. Scholars also debate whether a pure benefit or a balancing approach better follows *Press-Enterprise II*. *See* Levy, *supra* note 85, at 685.

99. *Compare In re* Search Warrant for Secretarial Area Outside Off. of Gunn, 855 F.2d 569, 570–72 (8th Cir. 1988) (considering news organization seeking pre-indictment access to search warrant materials for nationwide FBI investigation into corruption and fraud in procurement of military weapons systems, opposed by government and those being searched), *with* Times Mirror Co. v. United States, 873 F.2d 1210, 1211 (9th Cir. 1989) (considering different media organization seeking pre-indictment access to materials related to same investigation).

100. *In re Gunn*, 855 F.2d at 573.

101. *Times Mirror Co.*, 873 F.2d at 1215.

102. *In re Gunn*, 855 F.2d at 572–73 ("[P]ublic access . . . is important to the public's understanding of the function and operation of the judicial process and the criminal justice system and may operate as a curb on prosecutorial or judicial misconduct").

103. *In re* Search of Fair Fin., 692 F.3d 424, 432–33 (6th Cir. 2012) ("[The] monitoring of search warrant proceedings is already largely served . . . by the existence of remedies [for unconstitutional searches].").

in question,"[104] the Sixth Circuit considers not just the harms publicity could pose for a relevant investigation but also the harms publicity could cause to law enforcement more broadly.[105]

There are likely search warrants where publicity would be, on balance, beneficial, and others where it would be harmful. The disagreement on the functioning prong might result from the fact that courts must determine if a First Amendment right of access attaches to search warrants as an entire category. The Ninth Circuit has attempted to distinguish certain categories by refusing to recognize a First Amendment right of access to search warrants before an indictment but leaving open whether the right exists after an investigation or an indictment.[106] Some commentators have gone further, recommending that courts instead approach the functioning prong by deciding, on a case-by-case basis, whether to unseal a search warrant.[107]

c. Essential Closure and Narrow Tailoring

The strength of the First Amendment right of access, compared to the common law right, is that if the First Amendment right attaches to a particular category of documents, those seeking closure must meet a high bar of specific "findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest."[108]

In *Press-Enterprise II*, the Court only detailed that "higher values" might include a concern that access to a search warrant could compromise a defendant's constitutional rights to a fair trial.[109] But in *In re Gunn*, the "higher value" justifying sealing was the government's concern that unsealing the search warrant documents would hinder its investigations.[110] It is not entirely clear from *Press-Enterprise II* what interests represent the kind of higher value that justifies secrecy.[111]

Narrow tailoring may require a sealing court to explain why less restrictive alternatives, such as redaction, could not resolve secrecy

---

104. *Id*. at 429 (quoting Press-Enter. Co. v. Super. Ct. of Cal. for Riverside Cnty. (*Press-Enterprise II*), 478 U.S. 1, 8 (1986)).

105. *Id.* at 432 (considering impact on investigative tactics writ large).

106. *See Times Mirror Co.*, 873 F.2d at 1218; *see also* United States v. Bus. of Custer Battlefield Museum & Store Located at Interstate 90, Exit 514, S. of Billings, Mont., 658 F.3d 1188, 1196–97 (9th Cir. 2011) (declining to address question about rights of access after end of investigation).

107. *See* Levy, *supra* note 85, at 683–85 (proposing balancing approach similar to common law).

108. *Press-Enterprise II*, 478 U.S. at 9 (citing Press-Enter. Co. v. Super. Ct. of Cal., Riverside Cnty. (*Press-Enterprise I*), 464 U.S. 501, 510 (1984)).

109. *Id.* at 9.

110. *In re* Search Warrant for Secretarial Area Outside Off. of Gunn, 855 F.2d 569, 574 (8th Cir. 1988) ("There is a substantial probability that the government's on-going investigation would be severely compromised if the sealed documents were released.").

111. *Cf.* Levy, *supra* note 85, at 683–87 (arguing for categorical balancing test for "functioning" prong and individualized assessment of higher values).

concerns.[112] In *In re Gunn*, the Eighth Circuit reviewed the affidavits and other warrant materials and affirmed the district court's decision that "line-by-line redaction . . . was not practicable" because of frequent references to people other than the search's targets and information that "reveal[ed] the nature, scope and direction of the government's on-going investigation."[113]

Lawyers on both sides can struggle to contest the narrow tailoring requirement. As the Eighth Circuit explained, both lawyers might rely on "abstract and procedural" arguments "[b]ecause [petitioners are not] permitted to review the sealed documents," and the government "fear[s] [] disclosing [their] contents."[114] Although the Eighth Circuit concluded based on in camera review that releasing redacted affidavits was not practicable, one judge still believed portions could be released.[115] The limited opportunities to debate the narrow tailoring prong call into question the strength of the requirement.

Today, most circuits do not apply the First Amendment right of access to search warrants. Although circuits approach their analyses differently, litigants struggle to establish a historical tradition of openness and that the importance of public access outweighs the government's secrecy interests. Even in the Eighth Circuit, where the First Amendment right of access attaches to search warrants, the essential need and narrow tailoring requirements might not prove a particularly stringent standard for sealing.

For more than thirty years, scholars have criticized the right of access doctrines for failing to realize court transparency and government accountability.[116] These criticisms have proven especially accurate in attempts to unseal search warrant materials. The common law right often requires minimal explanation and thus imposes limited accountability. Moreover, the historically secretive nature of search warrant proceedings, paired with categorical consideration of the government's secrecy interests, hinder application of the stronger First Amendment right of access. As the next Part will explain, these barriers apply similarly even as new forms of electronic surveillance have emerged.

III. APPLYING RIGHTS OF ACCESS TO ELECTRONIC SEARCHES

Media and public interest organizations have relied on the public right of access doctrines to better understand how law enforcement conducts — and when courts allow — electronic surveillance. This Section

112. *See In re Gunn*, 855 F.2d at 574.
113. *Id.*
114. *Id.*
115. *See id.* at 576 (Heaney, J., concurring in part).
116. Bloch-Wehba, *supra* note 22, at 193–95; Hayes, *supra* note 22, at 1131–32; Poliak, *supra* note 23, at 1564.

focuses on two examples: *Electronic Frontier Foundation v. Superior Court of San Bernardino County*[117] and *In re Leopold to Unseal Electronic Surveillance Applications & Orders* (*In re Leopold III*).[118] These cases illustrate the types of information such organizations seek and the extent of variation that continues to exist in applying either the common law or the First Amendment rights of access. Ultimately, courts have struggled to accommodate the different forms of information that parties seek, and their underlying assumptions have diverged from a practical understanding of electronic surveillance and its harms.

A. Electronic Frontier Foundation v. Superior Court of San Bernardino County

Beginning in 2016, the California Electronic Communications Privacy Act requires law enforcement to secure a warrant for any electronic search and to disclose details of the warrant to the California Department of Justice if it was issued without informing the subject.[119] In 2018, *The Desert Sun*, relying on data that the California Department of Justice publishes, reported that San Bernardino County was almost twenty times as likely as other California counties to search its residents' electronic records or devices without their knowledge.[120] Between 2016 and 2018, the San Bernardino Sheriff's Department applied for more than 700 electronic search warrants, almost always under seal, and judges frequently granted an indefinite seal on the application materials.[121]

After *The Desert Sun*'s reporting, the Electronic Frontier Foundation ("EFF"), a digital civil liberties nonprofit,[122] sent public records requests to the Sheriff's Department.[123] EFF sought copies of six search warrant applications and orders.[124] The Sheriff's Department refused to disclose the materials because they had been sealed indefinitely by the

---

117. 299 Cal. Rptr. 3d 480 (Ct. App. 2022).

118. 964 F.3d 1121 (D.C. Cir. 2020). The discussion of the *In re Leopold* litigation also includes detailed analysis of the district court's approach in *In re Leopold to Unseal Certain Electronic Surveillance Applications & Orders* (*In re Leopold I*), 300 F. Supp. 3d 61 (D.D.C. 2018).

119. Christopher Damien & Evan Wyloge, *In San Bernardino County, You're 20 Times More Likely to Have Your Facebook, iPhone Secretly Probed by Police*, PALM SPRINGS DESERT SUN (Oct. 25, 2018, 9:30 AM), https://www.desertsun.com/story/news/2018/07/23/san-bernardino-countys-electronic-records-probed-most-california/820052002/ [https://perma.cc/629A-R8AR]; *see also* CAL. PENAL CODE § 1546.2(c) (West 2018).

120. *See* Brief of Plaintiff-Appellant at 13, Elec. Frontier Found. v. Super. Ct. of San Bernardino Cnty., 299 Cal. Rptr. 3d 480 (Ct. App. 2021) (No. E076778), 2021 WL 4202390, at *13 [hereinafter EFF Brief]; Damien & Wyloge, *supra* note 119.

121. *See* EFF Brief, *supra* note 120, at 13.

122. *See About EFF*, ELEC. FRONTIER FOUND., https://www.eff.org/about [https://perma.cc/VQA4-ARC2].

123. *See* EFF Brief, *supra* note 120, at 16.

124. *Id.*

issuing judges.[125] When EFF filed in California state court to enforce its public records requests, the court denied its motion to unseal the warrant materials.[126]

EFF then asked the court of appeals to unseal eight cell-site simulator warrants and affidavits.[127] EFF hoped to better understand the Sheriff's Department's and sealing judges' procedures, including (1) the offenses investigated, (2) the affiants' expertise, (3) explanations of how the searches would aid the investigation, (4) the nature of the information provided under the warrant, (5) how providers would comply, and (6) the reasons for seeking sealing.[128]

By January 2021, when the court held a hearing, the Sheriff's Department had executed all the warrants and completed all the related investigations.[129] But the trial court held that EFF had no right to access any of the affidavits and that, in the alternative, the Department's interests in protecting "confidential informant identity" and investigatory "sources and methods" were compelling.[130] After finding redaction infeasible, the court ordered that the affidavits, in their entirety, remain sealed indefinitely.[131]

EFF's arguments for unsealing the affidavits based on state law were unsuccessful.[132] The court rejected EFF's claim that the California Constitution's speech and transparency provisions created rights of access.[133] It further held that California Penal Code § 1534(a), which requires documents related to executed warrants to be made public ten days after their issuance,[134] and California Evidence Rules 2.550 and 2.551, which establish court sealing procedures, did not require disclosure in this case because California Evidence Code § 1040 and § 1041 allowed sealing to protect confidential informants or where disclosure

125. *Id.*

126. *Id.*

127. Elec. Frontier Found. v. Super. Ct. of San Bernardino Cnty., 299 Cal. Rptr. 3d 480, 486 (Ct. App. 2022).

128. *Id.*

129. *Id.* at 486–87.

130. *Id.*

131. *Id.*

132. *Id.* at 487–88.

133. *Id.* at 498–99 (finding that state constitutional speech protections were coextensive with First Amendment and that state constitutional transparency protections included an exception for statutes and rules "protecting the confidentiality of law enforcement and prosecution records") (quoting CAL. CONST. art. I, § 3(b)(5)). *But see* Petition for Review at 26, *Elec. Frontier Found. v. Super. Ct. of San Bernardino Cnty.*, 2023 Cal. LEXIS 103 (Sup. Ct. Jan. 11, 2023) (No. S277036) (disputing application of CAL. CONST. Art. I, § 3(b)(5)) [hereinafter Petition for Review].

134. *Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 487. The statute states: "The documents and records of the court relating to the warrant need not be open to the public until the execution and return of the warrant or the expiration of the 10-day period after issuance. Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record." CAL. PENAL CODE § 1534(a).

would otherwise be against public interests.[135] The court then turned to EFF's arguments that the First Amendment and common law rights of access required unsealing the affidavits.[136]

1. First Amendment

The court applied *Press-Enterprise II* to decide whether EFF had a First Amendment right of access to the search warrant affidavits.[137] On the history prong, EFF argued that California statutes, like CalECPA and § 1534(a) of the California Penal Code, which require some disclosures, created a tradition of public access to search warrant materials in California.[138] The court rejected this argument after concluding that the history prong considers "whether there is a longstanding *national* tradition of accessibility to the materials, not whether there is a California law-based tradition."[139]

The court then considered whether a national historical tradition existed. EFF cited the Ninth Circuit's decision in *Times Mirror*, which held that no First Amendment right existed pre-indictment, and the Eighth Circuit's decision in *In re Gunn*, which identified a First Amendment right of access.[140] San Bernardino County relied on the Sixth Circuit's decision in *Fair Finance*, which held there was no right to search warrant materials at any stage of an investigation.[141] Considering *In re Gunn* an outlier and finding *Times Mirror* avoided addressing post-indictment rights, the court held there was no historical tradition of access.[142]

The court noted that California courts can sometimes identify a First Amendment right of access without a historical tradition, if the

135. *See Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 492–93 (finding sealing court had properly applied exceptions in California Evidence Code Sections 1040–41 to affidavits at issue). *But see* Petition for Review, *supra* note 133, at 21, 24 (disputing sealing court's application of California Evidence Code Sections 1040–41 to California Penal Code § 1534(a) and California Rules of Court 2.550–2.551).

136. *Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 493, 499.

137. *Id.* at 493.

138. *Id.* at 494.

139. *Id.* (citing Press-Enter. Co. v. Super. Ct. of Cal. for Riverside Cnty. (*Press-Enterprise II*), 478 U.S. 1, 10 (1986) ("[T]he *near uniform* practice of state and federal courts has been to conduct preliminary hearings in open court.") (emphasis added by California court of appeal)) (emphasis in original).

140. *Id.* at 494–95. The court also rejected EFF's citation to *People v. Jackson*, 27 Cal. Rptr. 3d 596 (Ct. App. 2005), where a California court found a First Amendment right of access to sealed search warrant materials. *Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 493–94 (rejecting analogy because there, county never disputed newspaper's First Amendment right to documents post-indictment).

141. *Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 494–95.

142. *Id.*

functioning prong weighs in favor of disclosure.[143] But the court provided a long list of harms public access could pose to the search warrant application and criminal investigatory processes, including compromising information sources, confidential witness safety, government theories, or evidence.[144] The functioning prong, therefore, did not favor disclosure, so the First Amendment right of access did not attach.[145]

In the alternative, the court agreed with the trial court that the government demonstrated a compelling interest in keeping the affidavits sealed.[146] The trial court considered "protecting the identities of confidential informants and the confidentiality of law enforcement investigatory practices" to be a higher value justifying sealing.[147] Furthermore, the trial court rejected even partial redaction because the public could "piec[e] together other, unredacted information" and expose "confidential investigatory information."[148] After reviewing the affidavits, the appeals court affirmed the trial court's finding that "line-by-line redaction" was "not practicable" because redacting all the confidential information would "yield, at best, unintelligible paragraphs" with "little benefit to the functioning of the system."[149]

The appeals court found several reasons to reject EFF's First Amendment claim. The court did not find a clear direction in controlling precedent.[150] It additionally specified that any historical tradition must be national.[151] Unlike litigants in several of the circuit court cases, EFF did not seek detailed information on the content or strategy of any investigation, but rather a procedural understanding of how law enforcement conducted that investigation.[152] Nonetheless, the court

143. *Id.* at 496 ("EFF correctly notes, however, that even without a historical tradition of accessibility to search warrant materials, we may still find there is a First Amendment right to those materials based solely on *Press-Enterprise* [*II*]'s utility prong.") (citing NBC Subsidiary (KNBC-TV), Inc. v. Super. Ct. of L.A. Cnty., 980 P.2d 337, 362 n.32 (Cal. 1999) ("In any event, although evidence of such a historical tradition is a factor that strengthens the finding of a First Amendment right of access,[] the absence of explicit historical support would not, contrary to respondent's implicit premise, negate such a right of access." (citation omitted))).

144. *Id.* (quoting *In re* Search of Fair Fin., 692 F.3d 424, 432 (6th Cir. 2012)).

145. *Id.* at 496–97 (quoting *In re Fair Fin.*, 692 F.3d at 432).

146. *Id.*

147. *Id.* at 497.

148. *Id.* (citing People v. Jackson, 27 Cal. Rptr. 3d 596, 607 (Ct. App. 2005)).

149. *Id.* at 498 (quoting *In re* Search Warrant for Secretarial Area Outside Off. of Gunn, 855 F.2d 569, 574 (8th Cir. 1988) and *Jackson*, 27 Cal. Rptr. 3d at 609).

150. *Id.* at 494–95.

151. *Id.* at 494 (citing Press-Enter. Co. v. Super. Ct. of Cal. (*Press-Enterprise II*), 478 U.S. 1, 10 (1986)).

152. *Compare id.* at 486 (describing EFF's requests for cell-site simulator warrant applications), *with* Times Mirror Co. v. United States, 873 F.2d 1210, 1211, 1214 n.6 (9th Cir. 1989) (describing requests that could reveal the "nature and scope" of the Operation Ill-Wind investigation); *In re Gunn*, 855 F.2d at 571 (describing similarly revealing requests in same investigation); Balt. Sun Co. v. Goetz, 886 F.2d 60, 62 (4th Cir. 1989) (seeking to unseal warrant affidavits related to specific FBI investigation into healthcare insurance frauds).

interpreted "higher values" justifying sealing broadly, allowing sealing to preserve "confidentiality of law enforcement investigatory practices."[153] With such a broad interest, the court considered far more extensive redaction to be reasonable for its narrow tailoring analysis.[154] But even then, the court refused to release redacted documents because it believed those documents would not sufficiently benefit "the functioning of the system."[155]

In doing so, the court conflated the question of when the First Amendment right attaches with the question of narrow tailoring once it does. Moreover, it refused to release redacted documents based on its own judgment that they were too redacted to benefit the system as a whole, rather than considering EFF's or the public's interests in even a heavily redacted version.

2. Common Law

The court interpreted an understanding that the First Amendment right is stronger to imply that it is also broader, writing that "[c]ommon law rights provide the press and the public with less access than First Amendment rights."[156] Given its First Amendment holding, the court of appeals found that the trial court could not have abused its discretion and rejected a common law right of access.[157]

The appellate court's analysis reflects both continued variation in applying the common law and First Amendment rights and a court's discretion to narrow their scope.[158] One additional note: CalECPA provides powerful protections against electronic surveillance and explicitly provides for a form of openness. But it made no difference in this case, where the court refused to consider the common law right and rejected the statute's relevance to the First Amendment right as a non-national historical tradition.

153. *Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 497.

154. *See id.* at 497–98.

155. *See id.* at 498 (quoting United States v. Gonzales, 150 F.3d 1246, 1261 (10th Cir. 1998)).

156. *Id.* at 499 (citing Overstock.com, Inc. v. Goldman Sachs Grp., Inc., 180 Cal. Rptr. 3d 234, 251 (Ct. App. 2014)).

157. *Id.*

158. EFF appealed to the California Supreme Court, which declined to review the case. *See* Electronic Frontier Found. v. Super. Ct. of San Bernardino Cnty., S277036, 2023 Cal. LEXIS 103 (Jan. 11, 2023); *see also Results from the Petition Conference of 1/11/2023*, CAL. SUPREME CT. 2 (Jan. 11, 2023), https://supreme.courts.ca.gov/sites/default/files/supremecourt/default/documents/cr011123.pdf [https://perma.cc/8483-ABGB].

B. In re Leopold to Unseal Electronic Surveillance Applications and Orders

In 2013, Jason Leopold, a journalist at BuzzFeed News, asked the District Court for the District of Columbia to unseal federal government applications, orders, and docket numbers for "pen registers, trap and trace devices . . . , tracking devices, cell site location, stored email, telephone logs, and customer account records from electronic service providers" that were not related to an ongoing investigation.[159] He also requested a presumptive 180-day expiration date for related sealing orders.[160] Leopold later clarified that he did not seek any personally identifying information.[161]

The district court asked him to work with the U.S. Attorney's Office to refine his broad request.[162] During this process, the Reporters Committee for Freedom of the Press ("RCFP"), a nonprofit focused on advancing First Amendment and newsgathering rights, intervened.[163] After years of collaboration, Leopold, RCFP, and the U.S. Attorney's Office returned to the district court to request a hearing on whether the First Amendment or common law provided a right of access to documents for searches authorized under the Pen Register Act and the Stored Communications Act.[164] After the district court rejected claims for access under the First Amendment right and allowed only limited access under the common law right, Leopold and RCFP appealed to the D.C. Circuit.[165]

1. First Amendment

Although the D.C. Circuit avoided considering the First Amendment right on appeal,[166] the district court held that there was no First

159. *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold I*), 300 F. Supp. 3d 61, 68 (D.D.C. 2018) (quoting Pet. Unseal Records at 1, *In re Leopold I*, 300 F. Supp. 3d 61 (D.D.C. 2018) (No. 13–mc–00712) (also seeking list of docket numbers which typically remained under indefinite seal)).

160. *Id.*

161. *Id.* at 69.

162. *Id.* at 70.

163. *Id.* at 71; *What We Do*, REPORTERS COMM. FOR FREEDOM OF PRESS, https://www.rcfp.org/what-we-do/ [https://perma.cc/7X37-78PM].

164. *In re Leopold I*, 300 F. Supp. 3d at 79, 82.

165. On appeal, Leopold sought (1) "docket information for all SCA 2703(d) matters filed from 2008 to the present; (2) retrospectively, specified details to be extracted from 100% of pen register matters filed from 2008 to the present; and (3) prospectively, the presumptive unsealing at the close of investigations of applications (and supporting documents), orders, and docket entries for SCA warrants, SCA § 2703(d) orders, and pen register orders." *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold III*), 964 F.3d 1121, 1126 (D.C. Cir. 2020).

166. *Id.* at 1126–27 ("avoid[ing] unnecessarily passing on a constitutional question of first impression in th[e] circuit" because appellants indicated they believed they could receive relief under common law).

Amendment right of access to Pen Register and Stored Communications Act search materials.[167]

The district court concluded that, given the statutes' novelty, the documents could not have a historical tradition of openness, but it considered whether the statutes' text created that tradition.[168] The Pen Register Act directs courts to seal orders, and the Stored Communications Act either relieves government of any obligation to notify a customer about the compelled disclosure or allows the government to delay notification.[169] Both statutes also allow courts to issue orders preventing providers from disclosing the search to the targeted subscriber.[170] The district court concluded there was no tradition of openness because the statutes generally allowed the government to hide the search from potential targets.[171]

The district court also distinguished these statutory orders from traditional search warrants.[172] Because physical search warrants are executed with force and a physical intrusion, the court considered them a more "immediate and substantial invasion of privacy" than electronic searches, which the target may not even know occurred.[173]

2. Common Law

Reviewing the common law claims, the district court applied the D.C. Circuit's six-factor test to determine whether the balance of interests favored unsealing records.[174] The district court found that all six factors weighed in favor of retrospective access to documents, and that five of the six factors weighed in favor of prospective access.[175] But based on the "significant administrative burden" of unsealing the documents, the district court denied access to any past filings and allowed only limited releases from future filings.[176]

On appeal, the D.C. Circuit held that because the Stored Communications Act did not explicitly address sealing, the statute could not

---

167. *In re Leopold I*, 300 F. Supp. 3d at 108.

168. *Id.* at 86.

169. *Id.* at 83–85 (citing 18 U.S.C. § 3123(d)).

170. *Id.* (citing 18 U.S.C. §§ 2703(b)(1)(A), 2705(a), 2705(b)).

171. *Id.* at 86–87.

172. *Id.* at 87–88.

173. *Id.* at 88–89 (quoting *In re* Subpoena Duces Tecum, 228 F.3d 341, 348 (4th Cir. 2000)) (also considering that communications providers received notice and opportunity to challenge data requests).

174. *Id.* at 93–97; *see also supra* notes 52–53 and accompanying text.

175. *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold III*), 964 F.3d 1121, 1131 (D.C. Cir. 2020) (citing *In re Leopold I*, 300 F. Supp. 3d at 94–97 (finding that "the extent of previous public access to the documents" was the only factor that weighed against disclosure)).

176. *Id.* at 1126 (citing *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold II*), 327 F. Supp. 3d 1, 5, 21 (D.D.C. 2018)).

displace the common law right.[177] And, while the Pen Register Act's sealing directions displaced the common law presumption of access, it did not explicitly change the factors a court would consider.[178] After clarifying that the six-factor test may include weighing the administrative burden of release,[179] the D.C. Circuit remanded to the district court and explained that administrative burden "may not permanently foreclose their unsealing," even if it could "affect how and when judicial records may be released."[180]

On remand, the district court required the parties to jointly submit a status report with a specific proposal for implementing the D.C. Circuit's mandate.[181] In January 2022, the district court issued a standing order directing the court clerk to create annual public dockets that included unsealed and redacted warrants and orders filed under the Pen Register and Stored Communications Acts.[182] It also required the government to, at the close of each criminal investigation, prepare redacted versions of the underlying documents to be unsealed.[183]

Nearly ten years after Leopold's request, *In re Leopold I* resulted in success for transparency advocates. And the courts' analyses offer at least two avenues to strengthen the rights of access. Although the D.C. Circuit did not address the First Amendment right, the district court's willingness to consider a statute's text as providing a historical tradition suggests an opportunity for unsealing statutory warrants. The D.C. Circuit also did not elaborate on the district court's application of the six-factor test, but its clarification that administrative burden cannot be a reason to indefinitely refuse unsealing is helpful for parties seeking access.

The courts in *Electronic Frontier Foundation* and *In re Leopold I* and *III* interpreted the common law and First Amendment right of access doctrines very differently, which makes sense given the wide variation among courts. But, for the most part, the fact that the warrants and orders involved electronic searches did not change the courts' approaches.[184] In *In re Leopold I*, the district court did distinguish

177. *Id.* at 1129.

178. *Id.* at 1130.

179. *Id.* at 1132–33.

180. *Id.* at 1134.

181. *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold IV*), No. 13-mc-00712, 2020 WL 7481037, at *7 (D.D.C. Dec. 17, 2020).

182. *See* Standing Order at 1, *In re* Process for Public Docketing of Unsealed, Redacted Government Investigative Applications and Related Orders and Material (D.D.C. Jan. 25, 2022) (No. 22-05) [hereinafter Public Docketing Standing Order]; Samantha Reilly, *Federal Court Issues Win for Public Access, Ending Nine-Year Unsealing Effort by Journalist and Reporters Committee*, REPS. COMM. FOR FREEDOM OF PRESS (Apr. 11, 2022), https://www.rcfp.org/leopold-electronic-surveillance/ [https://perma.cc/K35P-NRCG].

183. *See* Public Docketing Standing Order, *supra* note 182, at 8–9.

184. This is with the obvious caveat that *In re Leopold III* considered statutory language in the Pen Register and Stored Communications Act because the procedures were mandated by those statutes. *See supra* text accompanying notes 169–72 and 177–81.

between ECPA-mandated orders and traditional search warrants, reasoning that electronic searches raised lesser privacy concerns because they lacked force or a physical intrusion, and could escape the target's knowledge.[185] Scholars might dispute the district court's conclusion and argue that more serious privacy concerns and secrecy cut in favor of providing access.[186] As the following Part will discuss, the Supreme Court adopted this view in recent opinions where it recognized the serious privacy implications of electronic surveillance, acknowledged a need for more government accountability, and ultimately distinguished between electronic searches and traditional physical ones.

IV. DISTINGUISHING ELECTRONIC WARRANTS

As technologies for electronic surveillance have advanced, there have been efforts to require law enforcement accountability by requiring search warrants, a requirement that necessarily precedes efforts to unseal those warrants. In considering whether surveillance constitutes a search — and therefore requires a warrant absent an exception — the Supreme Court recently distinguished between traditional surveillance and newer forms of electronic surveillance. In both *United States v. Jones*[187] and *Carpenter v. United States*, at least five Supreme Court justices called attention to the increased intrusiveness of electronic searches, the expansion of government surveillance capabilities, and the lack of public awareness of the surveillance.[188] The justices' reasoning also departed from traditional Fourth Amendment tests and introduced a new — and still uncertain — approach for courts to decide when government surveillance constitutes a search.

In 2012, the Supreme Court in *United States v. Jones* held that the government required a search warrant to install a GPS tracker on a person's car to monitor its movements over a four-week period.[189] Justice Sotomayor's concurrence considered the government's actions a search because they "enable[d] the government to ascertain, more or less at will," an individual's deeply personal information.[190] Because GPS monitoring, in comparison to physical surveillance, is "cheap" and "surreptitious[]," it "evade[d] the ordinary checks that constrain

185. *See In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold I*), 300 F. Supp. 3d 61, 87–89 (D.D.C. 2018).

186. *See supra* notes 1–8 and accompanying text (describing example technologies and harms).

187. 565 U.S. 400 (2012).

188. *See id.* at 415–16 (Sotomayor, J., concurring); *id.* at 429–30 (Alito, J., concurring); Carpenter v. United States, 138 S. Ct. 2206, 2220, 2223 (2018).

189. *Jones*, 565 U.S. at 404–06 (deciding question on trespass grounds).

190. *Id.* at 416 (Sotomayor, J., concurring) (including deeply personal information like "political and religious beliefs, sexual habits, and so on"); *see also* Kerr, *supra* note 15, at 328 (considering government's "more or less at will" capabilities the defining standard of Justice Sotomayor's concurrence).

abusive law enforcement practices: limited police resources and community hostility."[191] Justice Alito also concurred, but he considered the surveillance a search because, in his opinion, society did not expect that the government could collect detailed information over such a long period.[192] Although the two concurrences articulated distinct rationales, both rested on the way that GPS tracking increased the government's ability to collect private information.

In 2018, the Supreme Court reiterated these concerns when the majority opinion in *Carpenter* found that accessing cell-site location information over a four-month period without a warrant was unconstitutional.[193] Believing CSLI represented a "seismic shift[] in digital technology,"[194] Chief Justice Roberts considered the information collection a search based on "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[195]

These opinions reflect the Supreme Court's concerns about electronic surveillance: its privacy implications for people, the expanded opportunities for government collection, and the lack of public awareness.

First, the GPS tracking and CSLI collection at issue could expose intimate private details over long periods of time. Chief Justice Roberts and Justice Sotomayor shared concerns that these tools revealed not just a person's movements but also their intimate "familial, political, professional, religious, and sexual associations."[196] Justice Alito, too, appeared shocked by the GPS tracker's ability to collect, "monitor[,] and catalogue every single movement of an individual's car for a very long period."[197]

---

191. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring) (internal citation omitted).

192. *Id.* at 430 (Alito, J., concurring) ("For such offenses, society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual's car for a very long period."); *see also* Kerr, *supra* note 15, at 327 (describing how Justice Alito's opinion adopts the mosaic theory but relies on societal expectations of collective surveillance); *accord Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring) (also considering lack of reasonable expectation of this form of surveillance).

193. 138 S. Ct. 2206, 2217 (2018).

194. *Id.* at 2219; *see also* Tokson, *supra* note 10, at 6–7.

195. *Carpenter*, 138 S. Ct. at 2223, 2217 (explaining it "reveal[s] not only his particular movements, but through them his familial, political, professional, religious, and sexual associations" (internal citation omitted)); *see also* Tokson, *supra* note 10, at 6 (considering this language from the case to be the key doctrinal takeaway); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 378 (2019) (describing *Carpenter* test as "whether a given category of information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection").

196. *Carpenter*, 138 S. Ct. at 2217–19 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

197. *Jones*, 565 U.S. at 430 (Alito, J., concurring).

Second, the electronic surveillance tools enabled the government to collect more information about more people and do more with the information it collected. Because nearly every person has a phone, *Carpenter* worried that the government could track the movements of and constantly acquire this information about nearly any person, even those not under investigation.[198] Both Justice Alito and Justice Sotomayor described how GPS tracking allowed the government to not just collect information, but also record, aggregate, and analyze that information to apply it in new ways.[199] All three opinions also recognized that cost and labor limitations on traditional physical surveillance largely faded with electronic surveillance: physically following a target for a month drained police resources in ways that GPS tracking and requesting CSLI information did not.[200] Justice Sotomayor further worried that the government's capabilities would increase as technology advanced.[201]

Third, the three opinions shared a belief that people generally did not understand the extent of government surveillance capabilities.[202] Chief Justice Roberts and Justice Sotomayor questioned whether even a person aware of surveillance could avoid it, at least without compromising constitutional rights.[203] The collective public, too, might have limited options. As Justice Sotomayor wrote, "[B]ecause GPS monitoring . . . by design, proceeds surreptitiously, it evades [one of] the ordinary checks that constrain[s] abusive law enforcement practices: . . . community hostility."[204] Each person might not be able to avoid

198. *Carpenter*, 138 S. Ct. at 2218 ("[B]ecause location information is continually logged for all of the 400 million devices in the United States — not just those belonging to persons who might happen to come under investigation — this newfound tracking capacity runs against everyone."); *see also* Bloch-Wehba, *supra* note 10, at 27–28.

199. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring); *see* Kerr, *supra* note 15, at 332.

200. *See Carpenter*, 138 S. Ct. at 2217–18; *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring); *id.* at 429 (Alito, J., concurring) ("In the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. . . . Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."); *see also* Bloch-Wehba, *supra* note 10, at 29.

201. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (raising concerns that "[w]ith increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones").

202. *See Carpenter*, 138 S. Ct. at 2217 (finding government access to CSLI contravened reasonable expectation of privacy); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *Jones*, 565 U.S. at 430 (Alito, J., concurring).

203. *See Carpenter*, 138 S. Ct. at 2220 ("[I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

204. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring) (internal citation omitted); *see Carpenter*, 138 S. Ct. at 2217 ("For that reason, 'society's expectation has been that law

surveillance, and the secrecy means that it might be difficult to force practices to change.

Carpenter and the *Jones* concurrences represent a fundamentally different approach to Fourth Amendment search doctrine.[205] Courts traditionally approached surveillance sequentially by considering whether each discrete action a government actor took constituted a search.[206] But these three opinions focused on the "government conduct as a collective whole"[207] in what has been termed the "mosaic theory."[208] Professor Orin Kerr described the mosaic theory as asking whether, even if no discrete actions constitute a search, their aggregation "amount[s] to a search because their collection and subsequent analysis creates a revealing mosaic."[209]

The scope of the mosaic theory remains significantly unsettled and requires refining by courts or legislatures.[210] *Carpenter* indicates relevant factors that could amount to a multifactor test.[211] But *Carpenter* does not define the mosaic theory's boundaries; they could depend on the intrusiveness of the collected information, the duration or breadth of surveillance, or the technologies employed.[212] And the mosaic theory raises additional questions. How should courts weigh government

---

enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue.'" (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring))).

205. *See* Kerr, *supra* note 15, at 314 (describing as "major departure" that "implicate[s] fundamental questions about the future of Fourth Amendment law"); Ohm, *supra* note 195, at 360 (2019) ("*Carpenter* is an inflection point in the history of the Fourth Amendment.").

206. *See* Kerr, *supra* note 15, at 314.

207. *Id.* at 320.

208. *Id.* at 313.

209. *Id.* at 320.

210. *See id.* at 329 (describing as "exponentially more complicated" and requiring "creation of a parallel set of Fourth Amendment rules"); *cf.* United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.") (internal citation omitted); *see also* Taylor H. Wilson, Jr., *The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts*, 99 TEX. L. REV. ONLINE 155, 165 (2021) (summarizing varying lower court applications); Ben Vanston, *Putting Together the Pieces: The Mosaic Theory and Fourth Amendment Jurisprudence Since Carpenter*, 124 W. VA. L. REV. 657, 672–76 (2022) ("Most lower courts have rejected, either expressly or implicitly, the application of the mosaic theory to other contexts outside of CSLI technology.").

211. *See* Ohm, *supra* note 195, at 378 (describing *Carpenter* test); *cf.* Kerr, *supra* note 15, at 330–31 (criticizing "major ambiguities" within each Justice's opinions before *Carpenter*).

212. *See* Kerr, *supra* note 15, at 333–36 (wondering how to consider duration of surveillance, extent of information connected, technologies used, and combination of police approaches); *see also* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 51–57 (2020) (predicting applications in future cases); David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71–72 (2013) (arguing for focus on how information is gathered); Orin S. Kerr, Implementing *Carpenter*, THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 1, 28), https://ssrn.com/abstract=3301257 [https://perma.cc/2EUQ-5ZXV] (arguing for focus on the "use of a technology that *Carpenter* covers"); Ohm, *supra* note 195, at 378 (questioning what technologies *Carpenter* should cover).

actions that combine different technologies?[213] How should information collection relate to its recording and aggregation?[214] How would a search warrant articulate the particularity requirement for collection of information from various sources that become searches given their aggregation?[215]

Carpenter and the *Jones* concurrences create a new theory for how courts decide whether government surveillance constitutes a search and generally requires a warrant, and that theory appears to apply exclusively to electronic surveillance. In developing this mosaic theory, these opinions reflected the Court's serious concerns about electronic surveillance's privacy implications and capacity to increase government search power without public awareness or accountability. The warrant requirements imposed by *Carpenter* and *Jones* provide accountability for specific types of electronic surveillance by informing judges about law enforcement surveillance and requiring their approval.[216]

But the public also deserves to understand these practices and provide its input. As the next Part describes, the current common law and First Amendment right of access doctrines undervalue the public's interests in understanding electronic surveillance. Updating the rights of access is necessary for the public to participate in developing policy and other accountability mechanisms for electronic surveillance.

V. UPDATING THE RIGHTS OF ACCESS

Carpenter and the *Jones* concurrences recognize the differences between modern electronic surveillance and traditional forms of surveillance. As described by the Supreme Court, electronic surveillance implicates the public's interests through its expanded privacy intrusions, increased law enforcement secrecy, and an urgent need for policy. These factors should affect how courts consider whether to authorize warrants and whether those warrants, once authorized, should be unsealed.

This Part begins by exploring the extent to which the existing right of access doctrines can accommodate arguments about these features of electronic surveillance. It then proposes changes, both for courts applying the doctrines and policymakers drafting statutes.

---

213. *See* Kerr, *supra* note 15, at 335–36 (posing, as an example, location monitoring that relied on both cell-site tracking and GPS monitoring).

214. *See id*. at 331–33 (describing how mosaic theory expands scope of consideration beyond collection to analysis, use, and disclosure).

215. *See id.* at 338–39 (explaining that if mosaic theory depends on aggregation, the particularity requirement, which focuses on specifying a place or thing, does not easily translate).

216. *See* Bloch-Wehba, *supra* note 3, at 926–30.

A. Limits of Existing Doctrines

Today, the common law and First Amendment right of access doctrines seem to severely undervalue the public interests and to overvalue the government interests that are implicated by electronic surveillance. The common law right of access would allow — but often not require — a court to consider a changing balance of interests. But the First Amendment right of access's history prong, as courts have applied it to search warrants, likely precludes distinguishing search warrants based on the capabilities of modern search technologies.

The common law right relies on a court's balancing of the public's interest in access against interests in secrecy in each individual case. *Carpenter* and the *Jones* concurrences recognized several reasons the public has strong interests in understanding electronic searches, and those reasons strengthen the public interests in access to the warrants and related materials. First, expanding law enforcement's capacity to collect information from more people means that when the public seeks documents, it more often does so not only as observers but also as potential targets.[217] Second, unsealed search warrant materials provide greater public value because the gap between these technologies' capabilities and what people understand is greater.[218] Third, the public has a specific interest in contributing to necessary policy that regulates how law enforcement can use rapidly developing technologies.[219] Last, the public might have few alternatives to policy to avoid electronic surveillance or suppress the information.[220]

Electronic search warrants do not considerably increase legitimate secrecy interests.[221] Affidavits supporting them still rely on information from confidential informants or from third parties whose safety or reputations might be harmed by unsealing. The government might worry that disclosing an electronic search will reveal new technologies to the public and to those investigated.[222] Indeed, the court in *Electronic Frontier Foundation* did consider the government's interest in

---

217. *See supra* text accompanying notes 198–201 (describing concerns about scale of surveillance possible and decreasing cost and labor limitations on law enforcement).

218. *See supra* text accompanying notes 202–05 (describing both lack of public awareness and resulting inability to check government).

219. *See supra* text accompany notes 210–16 (describing mosaic theory's new approach and uncertainties requiring judicial or legislative definition).

220. *See supra* text accompanying notes 202–05 (describing inability to forgo technology that collects information or costs thereof). Defendants can attempt to apply the exclusionary rule to suppress information collected in violation of the Fourth Amendment, but non-defendants lack this form of remedy.

221. *See supra* text accompanying note 204 (describing secrecy concerns).

222. *See* Bloch-Wehba, *supra* note 22, at 185 ("[D]isclosure of a search performed in one criminal case risks exposing the new technique writ large, both to other targets of similar investigations but also to the public generally." (quoting Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 895 (2014))).

protecting the secrecy of law enforcement practices or strategy.[223] There should be a difference, however, between protecting government strategy for a particular case and hiding the nature of the technologies the government relies upon in many cases.

Although defendants' interests in secrecy likely do not change, their interests in public access might grow. Electronic searches, compared to physical searches, more easily evade a person's knowledge.[224] If a prosecutor does not bring charges, the defendant might never know the electronic search occurred.[225] In these cases, defense lawyers struggle to infer whether technologies like cell-site simulators were used at any point in an investigation.[226] Improving the public's understanding of the tools that police are using and in what situations they use them would help defendants identify and respond to their use.

Although increased public interest in access should push a court's balancing test toward unsealing electronic search warrant materials, the common law right delegates significant discretion to the sealing judge. In many circuits, sealing judges can adopt the government's factual claims, seal the decisions, and avoid considering redaction as a viable alternative.[227] And courts considering the common law right have discretion to order sealing without grappling with the ways that electronic surveillance may substantially increase the public's interests in access.[228]

The First Amendment right of access also struggles to accommodate differences between electronic and traditional searches. The emergence of extensive and invasive electronic search capabilities and the need for policy development might strengthen arguments under the functioning prong. But any distinctions between electronic and physical searches that focus on the nature of modern surveillance tools might limit a court's willingness to find a historical tradition of access.[229] This

223. Elec. Frontier Found. v. Super. Ct. of San Bernardino Cnty., 299 Cal. Rptr. 3d 480, 497 (Ct. App. 2022) (describing interest in protecting the "confidentiality of law enforcement investigatory practices").

224. *Cf.* Bloch-Wehba, *supra* note 3, at 934–35 (describing weakened notice requirements and comparing to "knock and announce" rule in physical searches of a home).

225. *Id.* at 937–39. Even if prosecutors do rely on an electronic search, defendants sometimes cannot access affidavits sealed to protect confidential informants. *See* People v. Hobbs, 873 P.2d 1246, 1259 (Cal. 1994) (adopting in camera review process that excludes defendants to review sealed affidavits for validity).

226. LYE, *supra* note 16, at 9–10.

227. *See* Section II.A.1.

228. *See* Sections II.A.1, III.A.2, III.B.2.

229. Courts' responses to claims that the First Amendment rights of access applied to video conference proceedings during the COVID-19 pandemic might help predict courts' responses to attempts to distinguish warrants for electronic surveillance. Considering the history prong, courts have ignored distinctions between traditional, in-person and newer, remote proceedings. *See* Courthouse News Serv. v. Forman, 606 F. Supp. 3d 1200, 1211 (N.D. Fla. 2022) (finding tradition of openness given uncontested declaration that "before e-filing [] newly

struggle to accommodate changing practices is one frequent criticism of the First Amendment's history prong.[230]

The existing right of access doctrines are insufficient to accommodate the greater public interests in unsealing electronic search warrants.

B. Updating the Rights of Access

Courts' applications of the rights of access to search warrants are particularly inconsistent.[231] But the common law and First Amendment right of access doctrines face criticisms beyond the search warrant context for failing to truly secure transparency of judicial records.[232] Although the common law right of access applies to all judicial records, its general balancing test does not provide strong protection for the right in practice.[233] The First Amendment right of access has limited scope and does not attach to many proceedings and documents.[234] Without adapting the history prong, in particular, the existing First Amendment right of access doctrine does not create much room to adapt to concerns around secrecy in electronic surveillance.[235]

With more consistent guidance for a sealing judge, the common law right of access could improve understanding of electronic surveillance, either by making it easier to unseal warrant materials or by requiring greater explanations of why courts cannot unseal them. The following paragraphs draw from various courts' examples to describe three guidelines for applying the common law right of access.

First, the test for a common law right of access could provide factors to measure the public interests. Although the common law test begins with the presumption of public interest in access, it also requires courts to compare public interests with secrecy interests.[236] It might help to provide factors by which courts can actually measure and

---

filed civil complaints were generally accessible"), *appeal dismissed voluntarily sub nom.* Courthouse News Serv. v. Broward Cnty. Clerk, No. 22-12288-HH, 2022 WL 9643634 (11th Cir. Sept. 6, 2022); United States v. Akhavan, 532 F. Supp. 3d 181, 186 (S.D.N.Y. 2021) (citing Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 93 (2d Cir. 2004)) (considering remote access during pandemic a "necessary corollary" of right to observe in-person proceedings). Some courts, acknowledging that new technologies lack historical traditions, have indicated their willingness to consider historical analogs. *See, e.g.*, Stevens v. Mich. State Ct. Admin. Off., No. 21-1727, 2022 WL 3500193, at *16–17 (6th Cir. Aug. 18, 2022) (indicating openness to flexible analogies of technology to historical practices but finding inadequate record to demonstrate tradition).

230. *See supra* text accompanying note 95 (questioning historical test's applicability to changing judicial practices).

231. *See* Sections II.A.1, II.B.1.

232. *See* Part II.

233. *See* Section II.A.1.

234. *See* Section II.B.1.

235. *Cf. In re* Search Warrant for Secretarial Area Outside Off. of Gunn, 855 F.2d 569, 574 (8th Cir. 1988) (finding First Amendment right attached but refusing to unseal).

236. *See* Section II.A.

explain the public interests. The D.C. Circuit describes possible factors with its six-factor test, which includes the public need, the extent of existing access, and the role documents played in a court's decision-making.[237] Courts might elaborate on the D.C. Circuit's consideration of public need and rely on additional factors, with particular poignance for claims to unseal electronic search warrant materials. For example, what is the existing baseline of public understanding, and how would these documents advance it? Assuming the records remain sealed, does the public have alternative avenues to gather this information? How much of the population does this information implicate, and how seriously? What democratic value, either in terms of policymaking or in terms of government accountability, does the use of this information further? Making these factors an explicit part of reviewing a common law right of access claim would make the public's interests in access more tangible, enabling a more meaningful comparison against the government's articulated interests.

The common law doctrine could similarly specify factors to better measure the government's interests. In particular, courts might probe the government's interest in protecting an ongoing investigation by questioning the investigation's stage and scope. Unsealing search warrant materials should be a lessening threat as a government investigation progresses. The government's interest in secrecy should decline after warrant execution and indictment, and it should be minimal post-conviction. Even if the government submits its explanation under seal, a court could consider how far the investigation reaches and how the warrant materials fit into it. Courts might also distinguish investigation-specific disclosures, which might warrant more secrecy, from law enforcement concerns about sharing the technologies they employ across many investigations.

The common law right of access should require courts to consider alternatives, namely, releasing redacted versions of warrants, affidavits, and applications. The Fourth Circuit reversed a sealing order because the sealing judge failed to consider the alternative of releasing a redacted version of the warrant materials.[238] Courts should also consider how public interests and secrecy interests compare because the secrecy interests will likely decline given the redactions. Although redacted versions will not offer as much information to the public, courts should not refuse to release those versions based on an assumption that they are insufficiently helpful.[239]

---

237. *In re* L.A. Times Commc'ns LLC, 28 F.4th 292, 297 (D.C. Cir. 2022).

238. Balt. Sun Co. v. Goetz, 886 F.2d 60, 63–66 (4th Cir. 1989).

239. *Cf.* Elec. Frontier Found. v. Super. Ct. of San Bernardino Cnty., 299 Cal. Rptr. 3d 480, 498 (Ct. App. 2022) (refusing access to redacted documents because they were effectively unintelligible and could serve "little benefit to the functioning of the system" (quoting United States v. Gonzales, 150 F.3d 1246, 1261 (10th Cir. 1998))).

Redaction is also a promising avenue because in cases like *Electronic Frontier Foundation* and *In re Leopold I*, litigants wanted to understand the structure of investigations rather than the content.[240] In many of the circuit court cases, litigants instead hoped to understand what the government was investigating.[241] Redacting the information needed to protect the ongoing investigation would likely remove more of the information valuable to those litigants. But, as the ultimate settlement of the *In re Leopold* litigation demonstrates, the government can redact warrant materials to protect confidential informants and ongoing investigations while still improving public understanding of how electronic surveillance works.[242]

For the First Amendment right of access, updating the history prong is necessary to expand the right to electronic search warrant materials. Here, courts' inconsistent approaches to *Press-Enterprise II*'s history prong could help.[243] The *Electronic Frontier Foundation* court refused to allow state statutes to create a tradition of openness.[244] But courts considering other proceedings and documents have held that state statutes guaranteeing access satisfied the history prong.[245] At least one court found a sufficient tradition of openness when documents were made public in four recent, similar cases.[246] And some courts have avoided the history prong altogether when a proceeding or document had conflicting or limited historical traditions.[247] Although not yet adopted to create a right of access to search warrants, these approaches

240. *See id.* at 486 (describing goals of unsealing request); *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold I*), 300 F. Supp. 3d 61, 68–69 (D.D.C. 2018) (describing unsealing request and clarification that no personal information was sought).

241. *See* Sections II.A.1, II.B.1.

242. *See* Public Docketing Standing Order, *supra* note 182, at 8–9.

243. *See* Section II.B.1.a; *see also* Poliak, *supra* note 23, at 1573 (summarizing courts' application of experience prong as eight distinct approaches to history).

244. *See Elec. Frontier Found.*, 299 Cal. Rptr. 3d at 494–95 (requiring a longstanding national tradition and rejecting arguments that CalECPA and Cal. Penal Code Section 1534(a) created a tradition of public access).

245. *See* Poliak, *supra* note 23, at 1577 (citing Whiteland Woods, L.P. v. Township of West Whiteland, 193 F.3d 177, 178–79 (3d Cir. 1999) (finding Pennsylvania Sunshine Act and Municipalities Planning Code guaranteed access to township planning commission meetings and satisfied experience prong) and Cal-Almond, Inc. v. U.S. Dep't of Agriculture, 960 F.2d 105, 106 (9th Cir. 1992) (finding several states' statutes providing for access to voter lists created tradition of public access)); *cf. In re Leopold I*, 300 F. Supp. 3d at 83–87 (concluding neither statute's text nor its historical application created tradition of openness for First Amendment right).

246. *See* Poliak, *supra* note 23, at 1577–78 (citing United States v. Erie Cnty., N.Y., 763 F.3d 235, 241–42 (2d Cir. 2014) (holding First Amendment right attached to monitor reports required by settlement agreement)).

247. *See id.* at 1579–80 (citing Detroit Free Press v. Ashcroft, 303 F.3d 681, 701, 705 (6th Cir. 2002) (finding deportation hearings had been at times both closed and opened and holding that First Amendment right attached)); *id.* at 1584–85 (citing United States v. Suarez, 880 F.2d 626, 631 (2d Cir. 1989) (recognizing First Amendment right despite lack of tradition of access to forms required by 1964 Criminal Justice Act)).

could support arguments that statutes, recent court decisions, or the novelty of electronic surveillance should satisfy the First Amendment's history prong.

Ultimately, both the common law and the First Amendment rights of access provide a baseline upon which statutes can strengthen rights of access. In applying both rights of access to warrants issued under the Electronic Communications Privacy Act ("ECPA"), courts have relied on ECPA's sealing and non-disclosure provisions in their decisions to maintain seals on search warrants.[248] Increasingly, policymakers will likely draft statutes that regulate how law enforcement can use various forms of electronic surveillance and establish new judicial authorization mechanisms.[249] In that process, they could also establish unsealing procedures that lay out a timeline for presumptive access after warrant execution or specific reasons why the government might retain a seal.

VI. CONCLUSION

New search technologies expand law enforcement's powers to investigate, monitor, and store information from many people over long periods of time. Today, government agencies can deploy these tools at minimal cost with minimal oversight. Courts and legislatures are beginning to recognize and respond to electronic surveillance's harms by requiring warrants or other forms of court authorization. But they should also value the role the public can play in accountability.

As a democratic ideal, transparency matters. Only by understanding how the government operates can people meaningfully participate in shaping policy. Transparency in search warrants and orders will empower people to push their governments to respond to electronic surveillance and to contribute to developing well-informed policy that addresses the many questions it raises. For example, which technologies should require warrants, and are there technologies so harmful society should ban them altogether? Are there distinct particularity and data management requirements that better map to digital searches? Should law enforcement's affidavits include more evidence to establish cause to collect the most personal data?

---

248. *See In re* N.Y. Times Co. to Unseal Wiretap & Search Warrant Materials, 577 F.3d 401, 404–11 (2d Cir. 2009) (refusing to unseal Wiretap Act warrants based on statute's "good cause" requirement); *see also In re* Leopold to Unseal Certain Elec. Surveillance Applications & Ords. (*In re Leopold III*), 964 F.3d 1121, 1129–30 (D.C. Cir. 2020) (considering SCA and Pen Register statute's text for whether they superseded common law right); *In re Leopold I*, 300 F. Supp. 3d at 83–87 (reading SCA and Pen Register statutes' non-disclosure provisions to suggest no tradition of openness for First Amendment right); *see also supra* note 14 (providing context on ECPA).

249. *See, e.g.*, CAL. PENAL CODE §§ 1546–1546.5 (West. 2015) (requiring warrant for any electronic search and requiring law enforcement to disclose details to California Department of Justice when warrant issued without informing target).

Today, the common law and First Amendment right of access doctrines undervalue the public benefit from government transparency. Adapting those doctrines to articulate why the public deserves to understand and define the limits of government's rationales for secrecy can be a first step towards creating appropriate policies for electronic surveillance.