**Washington Law Review**

Volume 93 | Number 1

3-1-2018

# Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders

Hannah Bloch-Wehba

# EXPOSING SECRET SEARCHES: A FIRST AMENDMENT RIGHT OF ACCESS TO ELECTRONIC SURVEILLANCE ORDERS

Hannah Bloch-Wehba*

*Abstract:* Although, as a rule, court proceedings and judicial records are presumptively open to the public, electronic surveillance documents are exceptions. Like ordinary search warrants, surveillance applications are considered ex parte. But court orders frequently remain sealed indefinitely, even when there is no basis for continued secrecy. Indeed, secrecy—in the form of gag orders, local judicial rules, and even clerical filing and docketing practices—is built into the laws that regulate electronic surveillance.

This Article argues that this widespread secrecy violates the First Amendment right of access to court proceedings and documents. The history of search and seizure shows that, far from requiring secrecy, searches and seizures were historically executed in public, with neighbors watching and even participating. Secrecy surrounding searches and seizures is a relatively new development, linked to the emergence of communications technology and laws governing the acquisition of customer records from third-party service providers. Transparency would play an especially positive role in this context because electronic surveillance is otherwise virtually insulated from public scrutiny: basic information about the scope of the government's authority to conduct surveillance and data regarding the frequency with which it does so is largely unavailable to the public. Sealing also obscures the government's interpretations of its own legal authority, as well as information about law enforcement technologies.

These twin arguments—historical and logical—establish a basis for courts to recognize that a First Amendment right of access attaches to surveillance materials after an investigation has concluded. While the government may have a compelling need for secrecy of surveillance materials in ongoing investigations, there is no government interest sufficiently compelling to warrant the sealing of tens of thousands of judicial documents long after an investigation has concluded.



---

* Clinical Lecturer in Law, Research Scholar, and Stanton First Amendment Fellow, Media Freedom & Information Access Clinic, Yale Law School. I am grateful for helpful comments and insights from Akhil Reed Amar, Jack Balkin, Vickie Baranetsky, Rebecca Crootof, Barry Friedman, Jameel Jaffer, Patrick Kabat, Heidi Kitrosser, John Langford, Jonathan Manes, Ashley Messenger, Lynn Oberlander, Riana Pfefferkorn, Cristina Rodríguez, Dave Schulz, and Andrew Selbst. This project also benefited from feedback from the fellows of the Information Society Project at Yale Law School and from participants at the 5th Annual Internet Law Scholars Works in Progress Conference and at Yale Law School's Free Expression Scholars Conference. Finally, the Article benefited tremendously from the careful efforts of the editors of the *Washington Law Review*. All errors are my own.

## INTRODUCTION

Every year, the government files thousands of ex parte applications seeking orders compelling communications service providers like Verizon, Sprint, AT&T, Facebook, Twitter, and Microsoft to provide access to customer records pursuant to the Pen/Trap Statute[1] and the Stored Communications Act (SCA).[2] The vast majority of the applications, and the orders granting them, are issued under seal.[3] Recent data suggests that, at least in some districts, only 0.1% of electronic surveillance requests ever become public.[4] Indeed, many of these

1. 18 U.S.C. § 3123 (2012).

2. *Id.* § 2703.

3. *See* TIM REAGAN & GEORGE CORT, FED. JUDICIAL CTR., SEALED CASES IN FEDERAL COURTS 21–22 (2009), http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf [https://perma.cc/2PM7-Y&MF] [hereinafter FJC STUDY].

4. *See* Spencer S. Hsu & Rachel Weiner, *U.S. Courts: Electronic Surveillance Up 500 Percent in D.C.-Area Since 2011, Almost All Sealed Cases*, WASH. POST (Oct. 24, 2016), http://wapo.st/2lgRxeW [https://perma.cc/BWJ9-YJAH].

applications and orders are made within entirely secret dockets unavailable to the public at all.[5] The recipients frequently receive gag orders directing them not to notify any person of the existence of the order.[6] While federal and state judges occasionally publish opinions in exceptional cases raising novel statutory issues, most of the requests are never acknowledged in published decisions. The result—an immense and growing docket of secret legal decisions issued in connection with criminal investigations.[7]

Many of these secret orders raise important constitutional and statutory issues. For example, does the Pen/Trap Statute authorize the use of a cell site simulator, sometimes also known as a stingray?[8] Only a few courts have issued public opinions explaining the legal authority for using stingrays to conduct communications surveillance.[9] One magistrate judge in the Northern District of Illinois, issuing an order imposing particular minimization requirements for the use of stingrays, noted that the "dearth of case law discussing these devices" prevented the court from even being aware of whether "judges may be allowing the

5. *See, e.g.*, Application of the Reporters Committee for Freedom of the Press to Unseal & for Other Appropriate Relief, *In re* Application of Jason Leopold to Unseal Certain Elec. Surveillance Applications & Orders, No. 1:13-mc-00712-BAH (D.D.C. Jan. 17, 2017), ECF No. 18 ("Such applications and orders are routinely maintained under seal indefinitely, even when the related investigation is no longer active, and are generally not reflected on publicly available court dockets.").

6. *See* 18 U.S.C. § 2705(b) (setting out requirements for separate nondisclosure order); *id.* § 3123(d) (requiring an order for installation and use of a pen register or trap and trace to direct that the recipient "not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court").

7. *See generally* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313 (2012); Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177 (2009).

8. Stingrays are devices that pose as cell towers, forcing nearby cell phones to connect, and monitor call information.

9. United States v. Tutis, 216 F. Supp. 3d 467, 484–85 (D.N.J. 2016) (denying motion to suppress evidence obtained after investigators obtained a communications data warrant authorizing use of a cell site simulator); United States v. Lambis, 197 F. Supp. 3d. 606, 614–16 (S.D.N.Y. 2016) (granting motion to suppress evidence obtained after DEA investigators obtained a pen register authorizing stingray use); *In re* The Application of the United States for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015) ("This opinion explains this Court's requirements relating to the use of cell-site simulators in a typical drug-trafficking investigation."); *In re* The Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) (requiring a search warrant for use of a stingray).

use of cell-site simulators without possessing a complete understanding of the device and how it works."[10]

New policing technologies like stingrays present urgent questions about how courts should apply legal protections in novel settings, but the public is frequently uncertain about the answers. What's more, those new technologies are only seldom regulated ex ante. Legislation prescribing, for example, how police use automated license plate readers, drones, x-ray backscatter vans, ShotSpotter systems, or facial recognition software is haphazard or nonexistent. Public debate about the appropriate use of these technologies is usually reactive, not proactive.

Against this background, the Pen/Trap Statute and the SCA stand apart: these statutes regulate when, how, and upon what standard police may acquire information about communications, directly from third-party service providers. Both federal and state law enforcement agencies rely on their ability to obtain information concerning electronic communications to investigate crimes ranging from Social Security Disability fraud[11] and robbery[12] to investigations of Wikileaks[13] and the Inauguration Day "riots."[14] These statutes govern how investigators can obtain both content and metadata of electronic communications, either in stored form or in real time.[15] Yet even though these techniques are subject to ex ante judicial review, they remain virtually insulated from public scrutiny and oversight.

Nor does the Fourth Amendment, which traditionally has regulated police investigations, appear to require much in the way of transparency. In general, the Fourth Amendment might require that police give notice when they execute a search or seizure warrant.[16] But the Constitution requires only that the person searched receive notice, not that the

10. 2015 WL 6871289, at *2.

11. *In re* 381 Search Warrants Directed to Facebook, Inc., 29 N.Y.3d 231, 239 (N.Y. 2017).

12. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

13. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283 (4th Cir. 2013).

14. Adam Edelman, *Feds Demand Facebook Share Information on Anti-Trump Protesters*, NBC NEWS (Sept. 29, 2017, 3:19 PM), https://www.nbcnews.com/politics/justice-department/feds-demand-facebook-share-information-anti-trump-protesters-n805801 [https://perma.cc/E6FH-PSQ7].

15. *See infra* tbl.1.

16. *See, e.g.*, City of W. Covina v. Perkins, 525 U.S. 234, 241 (1999) (requiring that law enforcement give property owners "[i]ndividualized notice" after property is seized); Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 PEPP. L. REV. 509, 527–28 (2014).

government notify the general public or otherwise expose its practices to public inspection. To the contrary, the United States Supreme Court has stated that the "success" of electronic surveillance "depends on secrecy."[17] Moreover, many communications surveillance scenarios involve no search warrant, and therefore no Fourth Amendment protections at all.[18]

Many scholars have grappled with critical substantive questions concerning the constitutionality of communications surveillance through the lens of the Fourth and Fifth Amendments.[19] Although warrantless communications surveillance of this type might violate substantive First Amendment rights,[20] and imposing gag orders may constitute an unlawful prior restraint,[21] only rarely have scholars focused on the secrecy of surveillance in ordinary criminal investigations as a substantive and procedural harm.[22]

The indefinite concealment from public view of electronic surveillance applications and orders violates the public's First Amendment right of access to judicial proceedings and documents and

17. Berger v. New York, 388 U.S. 41, 60 (1967).

18. Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (holding that individuals have no expectation of privacy in historical cell site location information obtained from service providers); *see also* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (same); United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) (same); United States v. Davis, 785 F.3d 498, 513 (11th Cir. 2015) (same), *cert. denied*, 136 S. Ct. 479 (2015); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (same).

19. *See, e.g.*, James X. Dempsey, *Keynote Address: The Path to ECPA Reform and the Implications of* United States v. Jones, 47 U.S.F. L. REV. 225 (2012); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1 (2013); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012); Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1 (2014).

20. Hannah Bloch-Wehba, *Process Without Procedure: National Security Letters and First Amendment Rights*, 49 SUFFOLK U. L. REV. 367 (2016); Gerald J. Votava III, *First Amendment Concerns in Governmental Acquisition and Analysis of Mobile Device Location Data*, 13 U. PITT. J. TECH. L. & POL'Y 1 (2013); Rebecca Wexler, Note, *Gags as Guidance: Expanding Notice of National Security Letter Investigations to Targets and the Public*, 31 BERKELEY TECH. L.J. 325 (2016).

21. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2330 (2014) ("[D]igital surveillance necessitates wide ranging use of prior restraint . . . .").

22. Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589 (2007); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843 (2014); *see also* Bloch-Wehba, *supra* note 20; Wexler, *supra* note 20.

endangers our ability to hold police accountable for their actions.[23] Part I of this Article evaluates the application of the First Amendment right of access to warrantless electronic surveillance orders. Under the First Amendment, the public has a qualified right of access to government proceedings and documents where there is a history of public access and where openness serves a positive function.[24] Appellate courts have split, however, regarding the application of this test to judicial proceedings that are the creation of statute and have little or no historical precedent.[25] Secrecy of electronic surveillance orders and applications also implicates recognized rights of access to docket sheets and judicial orders.

While secrecy now appears to be baked into huge swaths of investigative activity, historically this was not always the case. Section II.A illustrates how, at the framing of the Fourth Amendment, searches and seizures occurred in public, in real time and space, with neighbors and strangers watching and even participating as constables and customs officers rifled through homes, offices, and shops. The open and publicly accountable nature of searches and seizures was a key feature that fostered popular opposition to the scourges of general warrants and writs of assistance, promoted public understanding of the law of search and seizure, and ultimately led to the framers' adoption of the Fourth Amendment in order to restrain the government from warrantless and unreasonable searches and seizures.

Technological evolution prompted law enforcement investigations to become less transparent over time, as set forth in section II.B. Beginning with the Supreme Court's 1928 holding in *Olmstead v. United States*[26] that eavesdropping, without physical trespass, did not constitute a Fourth Amendment "search,"[27] investigations became much more opaque. Under the *Olmstead* holding and subsequent federal legislation, law enforcement was permitted to eavesdrop without a warrant—but was not allowed to use the evidence against a defendant in criminal

23. Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827 (2015).

24. Press-Enter. Co. v. Superior Court (*Press-Enterprise II*), 478 U.S. 1 (1986).

25. *Compare, e.g.*, *id.*, *and* United States v. Chagra, 701 F.2d 354, 363 (5th Cir. 1983) (recognizing that the fact that certain hearings have no historical counterpart does not preclude a right of access), *with In re* Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 291 (4th Cir. 2013), *and* United States v. El-Sayegh, 131 F.3d 158, 161 (D.C. Cir. 1997) (emphasizing the requirement of a history of access, even to novel proceedings).

26. 277 U.S. 438 (1928).

27. *Id.* at 466.

proceedings.[28] As a result, eavesdropping and wiretapping were occurring out of the eye of the public, unmoored from constitutional protections, and unmonitored by the courts. When, nearly half a century later, the Court held that the Fourth Amendment protects intangible conversations from unreasonable, unwarrantless searches,[29] the application of the warrant requirement should have brought searches back into the public eye. But instead, when Congress enacted legislation to govern electronic surveillance, protect individual rights, and regulate law enforcement, these laws frequently codified sweeping nondisclosure requirements as well.[30]

Making warrantless communications surveillance documents more transparent to the public also serves logical ends. Section III.A demonstrates that transparency of electronic surveillance applications and orders plays a critical role in ensuring the integrity of the process for authorizing surveillance and in the criminal justice process more broadly. Increasing transparency would boost the ability of judges, regulators, and the public to understand the methods, techniques, procedures, and legal reasoning that undergird communications surveillance. Even though the government applies for court orders ex parte, subjecting applications and orders to public scrutiny may deter police and prosecutorial misconduct. In addition, many of the traditional Fourth Amendment safeguards are absent in the statutory framework for electronic surveillance. The warrantless surveillance context lacks both ex ante safeguards like probable cause and prior notice, as well as the classic ex post remedy of exclusion.[31] In the Fourth Amendment setting, all three of these safeguards serve values of transparency by facilitating public scrutiny of the investigative process.

When police conduct, law enforcement tools, and the very rules that govern policing are cloaked in secrecy, it has systemic effects beyond a single defendant or criminal case, as set forth in section III.B. Law enforcement's failure to publicly acknowledge the use of new technologies keeps that technology out of the public eye and limits

---

28. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 28 (2004) (discussing the government's "aggressive interpretations" of the Communications Act of 1934, ch. 652, 48 Stat. 1064, 1100 (codified at 47 U.S.C. § 605 (1958) (amended 1968))).

29. Katz v. United States, 389 U.S. 347 (1967).

30. *See, e.g.*, 18 U.S.C. § 3123(d) (2012) (codifying sealing requirement in the Pen/Trap Statute); *id.* § 2518 (same, for Wiretap Act).

31. *See* United States v. Rigmaiden, No. 08-814-PHX-DGC, 2013 WL 1932800, at *10 (D. Ariz. May 8, 2013) ("Suppression is not an available remedy for violations of the SCA.").

debate about its appropriate use. The development of a secret body of law keeps judges from a full understanding of how to apply existing statutes and constitutional protections to new policing tools. The absence of even basic information about how frequently police use electronic surveillance tools makes it impossible to understand whether law enforcement is abusing its authority.

Part IV details why recognizing a right of access to electronic surveillance applications and orders strikes an appropriate balance between three competing objectives: law enforcement's need for secrecy, individual privacy, and the transparency essential to democratic accountability. Even if the First Amendment right of access attaches, it can be overcome if the government demonstrates that it has a compelling need for secrecy and the closure is narrowly tailored to meet that need. While the right of access might be overcome while an investigation is pending and surveillance is ongoing, changes in circumstances likely allow the applications and orders to become public later in time. Courts can also protect the privacy rights of individuals whose surveillance records may be unsealed through narrowly tailored redactions rather than wholesale secrecy. The classic methods of safeguarding private information in court filings—careful redactions and limitations on the duration of sealing—are equally useful in the surveillance context.

Electronic surveillance laws today have entrenched secrecy by design, limiting transparency in ways that hamper democratic accountability and impede public understanding of critical aspects of the criminal justice process. Secrecy is not just an accidental byproduct of the investigative process, but a sought-after result. Holding electronic surveillance to the same standards of transparency as physical searches would demonstrably improve the public's ability to hold police, prosecutors, and the courts accountable for the use—and misuse—of surveillance tools.

## I. THE RIGHT OF ACCESS IN THE ELECTRONIC SURVEILLANCE CONTEXT

Routine sealing of court records—including the court orders authorizing electronic surveillance—implicates the public's right of access to judicial records and proceedings.[32] So, too, do rules, practices, and procedures that impede access without meeting the appropriate common law and constitutional standards. While routine sealing in the

32. *See In re* Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008) (noting "[a]n indefinite non-disclosure order is tantamount to a permanent injunction of prior restraint" subject to the highest level of scrutiny).

electronic surveillance context remains commonplace in district courts throughout the nation, few litigants have challenged rules and practices requiring secrecy by seeking to vindicate a right of access under either the common law or the First Amendment.[33] This Part briefly outlines the contours of these two methods of ensuring access to judicial proceedings and documents, and then explores how the First Amendment right of access might be applied to electronic surveillance applications and orders.

### *A. The Common Law and Constitutional Right of Access to Judicial Proceedings and Documents*

In a series of cases during the 1970s and 1980s, the Supreme Court recognized public rights of access to court proceedings and documents grounded in the Constitution and the common law. In 1978, the Supreme Court found it "clear" that "the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents."[34] In *Nixon v. Warner Communications, Inc.*,[35] a group of broadcasters sought to obtain copies of twenty-two hours of the Nixon White House tape recordings that had been played in the courtroom during the Watergate trial.[36] The Court recognized that the recordings were precisely the type of "public records" to which a right of access attaches.[37]

When a party seeks access to a judicial record under the common law, the court is "faced with the task of weighing the interests advanced by the parties in light of the public interest and the duty of the courts."[38] On the side of disclosure, the *Nixon* Court found that a "newspaper publisher's intention to publish information concerning the operation of government" or "the citizen's desire to keep a watchful eye on the workings of public agencies" were interests sufficient to support access

33. *See, e.g.*, *In re* Petition of Jennifer Granick & Riana Pfefferkorn to Unseal Tech.-Assistance Orders & Materials, No. 16-mc-80206-KAW (N.D. Cal. Sept. 28, 2016) (seeking unsealing of surveillance orders and applications under the First Amendment); United States v. Pen Register, No. 2:10-mj-01235 (S.D. Tex. June 4, 2015) (intervening to unseal pen register application); *In re* The Application of Jason Leopold to Unseal Certain Elec. Surveillance Applications & Orders, No. 13-712 (D.D.C. Aug. 23, 2013) (seeking unsealing of pen register and trap and trace applications and orders under the First Amendment).

34. Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978).

35. 435 U.S. 589 (1978).

36. *Id.* at 594.

37. *Id.* at 597.

38. *Id.* at 602.

to judicial documents.[39] Among the countervailing interests were the disgraced President Nixon's own property and privacy interests in the recordings, as well as his desire that the tapes not be commercialized.[40]

The *Nixon* Court ultimately dodged the balancing inquiry by holding that the Presidential Recordings Act provided an alternative for gaining access to the records at issue in the case.[41] It concluded, nonetheless, that "any access scheme finally implemented" under the Act would still need to satisfy statutory and constitutional requirements.[42]

As the balance of interests in the *Nixon* case suggests, the common law presumption of access to judicial documents "can be overcome by a competing, but not necessarily a constitutionally compelled, interest."[43] Likewise, courts "cannot craft federal common law when Congress has spoken directly to the issue at hand."[44] As a result, a common law right of access may be displaced or superseded by a statute that provides a substitute disclosure scheme or advances a sufficiently weighty interest in closure.[45] For example, the D.C. Circuit has indicated that the common law right of access to hearings and materials related to a grand jury investigation, if any existed, would have been "supplanted" by Rule 6(e) of the Federal Rules of Criminal Procedure.[46]

After *Nixon*, the Court recognized that the Constitution imposes an even higher standard upon interference with the public's right to attend certain government proceedings. The First Amendment confers a public right of access to a variety of criminal proceedings—including trials,[47] voir dire,[48] and preliminary hearings.[49] Under the First Amendment, as

---

39. *Id.* at 597–99.

40. *Id.* at 601–02; *see also* United States v. Hubbard, 650 F.2d 293, 317–21 (D.C. Cir. 1980) (articulating six factors for courts to weigh in considering whether to unseal judicial documents).

41. *Nixon*, 435 U.S. at 603–07.

42. *Id.* at 607–08.

43. Lynn B. Oberlander, *A First Amendment Right of Access to Affidavits in Support of Search Warrants*, 90 COLUM. L. REV. 2216, 2217 (1990).

44. Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 937 (D.C. Cir. 2003).

45. *See, e.g.*, United States v. Gonzales, 150 F.3d 1246, 1263 (10th Cir. 1998) (explaining that the rules related to the release of information under the Criminal Justice Act "occupy this field and would supercede the common law right even if one existed"); *see also* MetLife, Inc. v. Fin. Stability Oversight Council, 865 F.3d 661, 669 (D.C. Cir. 2017) (holding that the Dodd-Frank Act does not "categorically bar disclosure by courts" of financial information in briefs and other court documents).

46. *In re* Motions of Dow Jones & Co., 142 F.3d 496, 504 (D.C. Cir. 1998).

47. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).

48. Press-Enter. Co. v. Superior Court (*Press-Enterprise I*), 464 U.S. 501 (1984).

49. *Press-Enterprise II*, 478 U.S. 1 (1986).

the Supreme Court recognized in *Press-Enterprise v. Superior Court of California* (*Press-Enterprise II*),[50] a court considering an access claim must assess both "whether public access plays a significant positive role in the functioning of the particular process in question" and "whether the place and process have historically been open to the press and general public."[51]

If the First Amendment right attaches, the standard for closure is far more demanding than under the common law: "[t]he presumption of openness may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest."[52] This more robust standard guides courts when they consider whether statutes limiting access comply with the Constitution. Any statute that purports to supplant the common-law right of access remains subject to the requirements of the First Amendment if it limits the ability to view and inspect records or proceedings to which the public has a *constitutional* right.

In fact, the First Amendment right of access evolved out of the close relationship between judicial transparency, criminal justice, and democratic oversight. In 1979, the Supreme Court—while holding that the Sixth Amendment did not guarantee a public right of access to criminal trials—indicated that there might be a right of access to criminal trials couched in the First and Fourteenth Amendments.[53] The Court soon explicitly recognized the First Amendment right of access to criminal trials, holding in *Richmond Newspapers*[54] in 1980 that "the right to attend criminal trials is implicit in the guarantees of the First Amendment; without the freedom to attend such trials, which people have exercised for centuries, important aspects of freedom of speech and of the press could be eviscerated."[55]

In his concurrence, Justice Brennan identified "two helpful principles" to cabin the application of the right of access.[56] First, Brennan emphasized the importance of history, writing that "the case for a right of access has special force when drawn from an enduring and vital tradition of public entree to particular proceedings or information,"

50. 478 U.S. 1 (1986).

51. *Id.* at 8.

52. *Press-Enterprise I*, 464 U.S. at 510.

53. Gannett Co. v. DePasquale, 443 U.S. 368, 391–92 (1979).

54. 448 U.S. 555 (1980).

55. *Id.* at 580 (citations and quotation marks omitted).

56. *Id.* at 589 (Brennan, J., concurring).

and that "what is crucial in individual cases is whether access to a particular government process is important in terms of that very process."[57] Second, Brennan recognized that the right of access to government proceedings served an important functional end as a critical feature of the First Amendment's "*structural* role . . . in securing and fostering our republican system of self-government."[58] Far from being limited to criminal trials, Brennan wrote, the structural model of press freedom stemmed from the right to gather information—and "the stretch of this protection is theoretically endless."[59]

In the 1982 *Globe Newspaper* case,[60] the Court returned to Brennan's two-pronged approach, examining both the history of openness as well as the positive results that transparency yields. The Court struck down a Massachusetts law that "*required* the closure of sex-offense trials only during the testimony of minor victims,"[61] elaborating on the reasons that access to criminal trials is so crucial. First, the Court found that the historical "presumption of openness"[62] was virtually uninterrupted, a fact that "implies the favorable judgment of experience."[63] Second, public access leads to positive outcomes, the Court wrote: "[p]ublic scrutiny of a criminal trial enhances the quality and safeguards the integrity of the factfinding process . . . [and] fosters an appearance of fairness, thereby heightening public respect for the judicial process."[64] Although the Court recognized that the constitutional right of access to criminal trials is "not absolute," it held that when the government attempts to deny access, "it must be shown that the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest."[65]

Two years later, the Court expanded the constitutional right of access from criminal trials to other judicial proceedings. In *Press-Enterprise Co. v. Superior Court of California* (*Press-Enterprise I*),[66] the Court held that the First Amendment guarantees the right to attend voir dire.[67] Looking to the "presumptive openness of the jury selection process" in

57. *Id.*
58. *Id.* at 587 (Brennan, J., concurring).
59. *Id.* at 588 (citing William J. Brennan, *Address*, 32 RUTGERS L. REV. 173, 176 (1979)).
60. Globe Newspaper Co. v. Super. Ct. for Norfolk Cty., 457 U.S. 596 (1982).
61. *Id.* at 600.
62. *Id.* at 605.
63. *Id.* (quotation marks omitted).
64. *Id.* at 606.
65. *Id.* at 606–07.
66. 464 U.S. 501 (1984).
67. *Id.*

England both before and after the Norman Conquest, the Court determined that "[p]ublic jury selection thus was the common practice in America when the Constitution was adopted."[68] The public face of the criminal justice process "gave assurance to those not attending trials that others were able to observe the proceedings and enhanced public confidence."[69]

Based both on this historical experience as well as its apparently positive outcome, the Court concluded, "[c]losed proceedings, although not absolutely precluded, must be rare and only for cause shown that outweighs the value of openness."[70] The Court emphasized that the standard for closing proceedings was extraordinarily demanding: "[t]he presumption of openness may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest."[71]

Finally, in 1986, the Court considered whether a First Amendment right of access attaches to preliminary hearings in criminal prosecutions.[72] Recognizing that the preceding decisions had "emphasized two complementary considerations,"[73] the *Press-Enterprise II* Court articulated a two-prong test for whether the right of access attaches to a particular proceeding. A court considering an access claim must assess both "whether public access plays a significant positive role in the functioning of the particular process in question" and "whether the place and process have historically been open to the press and general public."[74]

None of these cases overtly restricted the First Amendment right of access to judicial proceedings. Rather, in *Press-Enterprise II*, the Court referred to "governmental processes."[75] And, indeed, appellate courts have since found that the First Amendment right of access applies broadly: to administrative proceedings,[76] classified evidence in habeas hearings brought by detainees at Guantánamo Bay,[77] horse roundups,[78]

---

68. *Id.* at 508.

69. *Id.* at 507.

70. *Id.* at 509.

71. *Id.* at 510.

72. *Press-Enterprise II*, 478 U.S. 1, 10 (1986).

73. *Id.* at 8.

74. *Id.*

75. *Id.*

76. Whiteland Woods, L.P. v. Township of W. Whiteland, 193 F.3d 177, 181 (3d Cir. 1999).

77. Dhiab v. Obama, 70 F. Supp. 3d 486 (D.D.C. 2014), *rev'd sub nom.* Dhiab v. Trump, 852 F.3d 1087 (D.C. Cir. 2017).

and executions.[79] While the constitutional right of access is expansive, however, it is not limitless. As the Supreme Court has recognized, the presumption of openness may be overcome based on a compelling government interest, which "is to be articulated along with findings specific enough that a reviewing court can determine whether the closure order was properly entered."[80]

### *B. Closure and Surveillance*

A variety of statutes regulate how the government can obtain content and metadata from third-party service providers. The SCA permits the government to apply for a court order requiring a communications service provider to disclose either stored communications content (e.g., emails or messaging transcripts) or metadata (e.g., "to" and "from" information).[81] When the government seeks a search warrant for stored communications, it must follow the procedures in Rule 41 of the Federal Rules of Criminal Procedure, which governs search warrant practice as a general matter.[82] The Pen/Trap Statute permits the government to apply for a court order requiring a communications service provider to assist in placing a pen register or trap and trace device on a communications line to monitor metadata in real time.[83] Lastly, the Wiretap Act, also known as "Title III," authorizes the government to seek an order to intercept wire, oral, or electronic communications in real time.[84]

All three statutes include provisions that flout the norms of court openness. The Pen/Trap Statute requires that an "order" should be sealed,[85] while Title III requires the sealing of applications and orders

78. Leigh v. Salazar, 677 F.3d 892 (9th Cir. 2012).

79. Cal. First Amendment Coal. v. Woodford, 299 F.3d 868 (9th Cir. 2002).

80. *Press-Enterprise I*, 464 U.S. 501, 510 (1984).

81. 18 U.S.C. § 2703 (2012). While the SCA does not always require law enforcement to get a warrant for content, the Sixth Circuit and numerous lower courts have held that the Fourth Amendment protects the content of emails. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); *see also* JENNIFER R. HENRICHSEN & HANNAH BLOCH-WEHBA, ELECTRONIC COMMUNICATIONS SURVEILLANCE: WHAT JOURNALISTS AND MEDIA ORGANIZATIONS NEED TO KNOW 5 n.18 (2017), https://www.rcfp.org/rcfp/orders/docs/SURVEILLANCE.pdf [https://perma.cc/6AK5-CYFW].

82. 18 U.S.C. § 2703(a); FED. R. CRIM. P. 41.

83. Pen registers are devices that can record "dialing, routing, addressing, or signaling information" for outgoing communications, such as the phone numbers for outgoing calls. 18 U.S.C. § 3127(3). Trap and trace devices record the same information for incoming communications. *Id.* § 3127(4).

84. *Id.* §§ 2510–2522.

85. *Id.* § 3123.

(as well as any recordings made during the period of the wiretap).[86] These sealing provisions direct courts to maintain the documents in a manner that prevents the public, or other parties, from accessing them. In contrast, neither the SCA nor Rule 41 includes any provisions authorizing sealing of judicial records. Instead, both authorities include provisions requiring notification of the affected individual as a general rule, but permitting the government to delay notice if a court finds "reason to believe" that notice "*may* have an adverse result."[87] In its most recent report, the Administrative Office of the U.S. Courts tallies a total of 14,801 applications for delayed notice search warrants, and extensions thereof, in fiscal year 2015. [88] All but twenty-eight applications were granted.[89] Over 80% of the applications were issued in connection with investigations of drug crimes.[90]

The SCA also permits the government to apply for a separate court order "commanding" the recipient of an SCA warrant or subpoena not to notify any person of the existence of the order.[91] This "secrecy order" provision requires that a court find "reason to believe that notification of the existence of the warrant, subpoena, or court order *will* result in" one of the enumerated harms.[92]

So-called "secrecy orders" are distinct from sealing provisions; they are not instructions to courts, but rather restraints upon recipients—private companies and individuals—that prevent them from speaking to the public. Secrecy orders thus raise an additional First Amendment concern, because they constitute prior restraints on the First Amendment rights of the recipients, who may wish to speak about the orders they have received.[93] While the government does not disclose the number of

86. *Id.* § 2518.

87. *Id.* § 2705(a)(1)(A) (emphasis added). The enumerated "adverse result[s]" are the following: "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." *Id.* § 2705(a)(2).

88. ADMIN. OFFICE OF THE U.S. COURTS, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR DELAYED-NOTICE SEARCH WARRANTS AND EXTENSIONS (2015), http://www.uscourts.gov/file/20408/download [https://perma.cc/5RHD-XMUQ].

89. *Id.*

90. *Id.*

91. 18 U.S.C. § 2705(b).

92. *Id.* (emphasis added).

93. Prior restraints are "administrative and judicial orders *forbidding* certain communications when issued in advance of the time that such communications are to occur." Alexander v. United States, 509 U.S. 544, 550 (1993).

secrecy orders sought each year,[94] Microsoft, in recent litigation, has claimed that it received over 3,250 secrecy orders over a twenty-month period alone.[95] In response to Microsoft's lawsuit, the Department of Justice recently adopted a new policy that will require each secrecy order to have "an appropriate factual basis" and presumes that, "[b]arring exceptional circumstances," a secrecy order should last no longer than one year.[96]

**Table 1:**
**Surveillance Authorities and Sealing Provisions**

| | **Type of information sought** | **Notice provision** | **Gag provision** |
|---|---|---|---|
| **Electronic Search Warrant** | Communications content, metadata, and/or basic subscriber and session information | No notice required. 18 U.S.C. § 2703(b)(1)(A) | 18 U.S.C. § 2705 |
| **2703(d) Order** | Communications content (opened, sent, or older than 180 days) | Notice required, but may be delayed. | 18 U.S.C. § 2705 |
| | Basic subscriber and session information; communications metadata | No notice required. 18 U.S.C. § 2703(c)(3) | 18 U.S.C. § 2705 |
| **Pen/Trap Order** | Dialing, routing, addressing, or signaling information | No notice required. | 18 U.S.C. § 3123(d) |
| **Title III Order** | Communications content | Notice required. 18 U.S.C. § 2518(8)(d) | 18 U.S.C. § 2511(1)(e) |

94. *See infra* section III.D.

95. First Amended Complaint for Declaratory Judgement at ¶ 5, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d. 887 (W.D. Wash. 2017) (No. 2:16-cv-00538-JLR), ECF No. 28.

96. U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., POLICY REGARDING APPLICATIONS FOR PROTECTIVE ORDERS PURSUANT TO 18 U.S.C. § 2705(B) (2017), https://www.justice.gov/criminal-ccips/page/file/1005791/download [https://perma.cc/4VLZ-CXSE].

### *1. Secrecy's Widespread Impact*

As a result of the sealing, non-disclosure, and delayed-notice provisions codified in federal surveillance law, secrecy is now a condition endemic to the federal courts.[97] A 2009 study found that, in the year 2006, over 15,000 sealed magistrate judge cases were filed, 83% of which were "warrant-type applications."[98] Of the "warrant-type applications," 54% were search warrants, and 37% were applications for pen registers, trap and traces, tracking devices, "and the like."[99] The study suggests that in the year 2006, the government filed 7,486 applications in the federal courts for pen registers, trap and traces, tracking devices, and other court orders compelling disclosure of communications metadata—all of which were entirely secret.[100] To put this in perspective, the Administrative Office of the U.S. Courts reports that in the twelve-month period ending in September 2006, magistrate judges handled a total of 32,467 search warrants;[101] the study reports that some 7,400 sealed cases were search warrants.[102] Over 22% of the search warrants issued in 2006 were entirely sealed.[103]

Today, it appears that government is compelling companies to disclose user information at rates never before seen. The Administrative Office of the U.S. Courts reports that federal magistrate judges considered 72,960 applications for search warrants in the fiscal year ending in September 2016, over twice as many as in 2007.[104] Technology companies and communications providers now receive tens

---

97. *See* Smith, *Gagged, Sealed & Delivered*, *supra* note 7.

98. FJC STUDY, *supra* note 3, at 21–22.

99. *Id.* at 22. In addition, 8,121 sealed "miscellaneous cases" were filed that year, 58% of which were warrant-type applications. *Id.* at 23.

100. *Id.* at 21–22. It is possible that the FJC Study was in fact underinclusive, since the study accounted only for cases that were entirely sealed, and did not analyze sealed documents in unsealed cases. *See id.* at 1 ("We did not count as sealed cases those with every document sealed and only highly redacted docket sheets available on PACER, because a method different from the one we used would be necessary to find all such cases.").

101. ADMIN. OFFICE OF THE U.S. COURTS, JUDICIAL BUSINESS TABLE S-17, 2 (2006), http://www.uscourts.gov/file/13538/download [https://perma.cc/2EK9-L7VT].

102. FJC Study, *supra* note 3, at 23.

103. This Article's focus on federal courts is not meant to distract from similar issues facing state courts. State courts may issue orders under the Pen/Trap Act, 18 U.S.C. § 3122, and the Stored Communications Act, 18 U.S.C. § 2703. If anything, disparities in record-keeping and electronic docketing practices in state courts make it even more difficult to investigate and uncover sealing problems than in federal courts. Due to the lack of available data, however, the Article leaves for another day discussion of sealing issues in state courts.

104. ADMIN. OFFICE OF THE U.S. COURTS, JUDICIAL BUSINESS TABLE S-17 (2016), http://www.uscourts.gov/file/21849/download [https://perma.cc/HJ7U0AR8S].

of thousands of government demands each year: Verizon received over 21,000 search warrants in 2016.[105] That number pales in comparison to the number of warrantless requests demanding non-content information, which far exceeds the number of search warrants.[106] Facebook has reported that approximately 57% of the tens of thousands of law enforcement requests the company receives come with gag orders.[107]

### *2. Secrecy in Judicial Administration*

Local judicial rules compound prosecutorial habit and the secrecy provisions in electronic surveillance statutes, giving rise to a system in which the government routinely applies for electronic surveillance orders in secret dockets, under complete seal. Given the overlapping and inconsistent provisions in electronic surveillance statutes, it is perhaps not surprising that district courts also exhibit inconsistencies in docketing applications for electronic surveillance. For example, some districts classify search warrants as "criminal," others "miscellaneous," and still other districts as "magistrate" cases.[108] In addition, "[t]hree districts used 'sw' as a case type for search or seizure warrants," and one district used "pr" as a case type for pen registers.[109]

Many district courts have local rules that reflect a default presumption of secrecy. Some districts provide for routine sealing of documents filed in connection with applications for electronic surveillance.[110] For example, the District of Minnesota requires applications for electronic surveillance to be made under seal and bars unsealing "except by court order."[111] Broad default sealing requirements result in more documents being filed under seal than requirements that the government apply for individual court orders each time it seeks to seal information.

---

105. *United States Report*, VERIZON, http://vz.to/2lMOyb5 [https://perma.cc/M2KW-YXVA].

106. *Id.* (showing that Verizon received over 32,000 non-search warrant orders).

107. *Transparency Report*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2016-H2/ [https://perma.cc/VWF7-CYF8].

108. FJC Study, *supra* note 3, at 2.

109. *Id.* at 27.

110. D. D.C. CT. R. 49(e) (requiring that applications for electronic surveillance be filed under seal, but not requiring a motion to seal); D. CONN. C.P.L.R. 57 (providing that orders authorizing a pen register or trap and trace are filed in a "miscellaneous sealed case"). However, the Connecticut rule differs for search warrant returns: "[u]nless otherwise directed by the Court for sufficient cause, search warrant returns shall be docketed as unsealed filings." *Id.*; *see also* Memorandum from Andrew Udelsman & Yurij Melnyk, Media Freedom & Info. Access Clinic, to Janet C. Hall, Chief Judge, D.D.C. (Apr. 27, 2017), https://law.yale.edu/system/files/area/center/mfia/document/2017.04.27_ mfia_scrap_ct_letter_final.pdf [https://perma.cc/7R9B-AQLV].

111. D. MINN. L. R. 49.1.

Electronically docketing surveillance materials also materially improves the public's practical ability to gain access to information, but many districts nonetheless require surveillance applications to be filed only in paper form. In the Eastern District of Virginia, District of Columbia, and many other districts, search warrants and pen registers are filed in paper and never made available electronically.[112] Electronic filing and docketing practices were adopted, not to facilitate access by the public, but rather because improvements in cost and efficiency offered "major gains for judges and court administrators."[113] Electronic docketing, however, has also fundamentally changed researchers' ability to access court data.[114] Jurisdictions that exempt surveillance orders from electronic filing forego gains in efficiency as well as in public accountability. Judicial districts that exempt electronic surveillance documents from e-filing choose not to avail themselves of an automated system reminding the government that it must meet an affirmative obligation in order to maintain a record under seal. As a result, secret orders may fly under the radar of the courts and the public.

District courts can also reduce the scope and extent of sealing if they adopt default rules regarding judicial oversight or review of secrecy requirements. Although electronic surveillance laws might require that applications be filed under seal as an initial matter, they also anticipate that secrecy need not last forever.[115] Local rules also can trigger mandatory action by the court or by prosecutors to review and, if

---

112. U.S. DIST. COURT E. DIST. OF VA., EASTERN DISTRICT OF VIRGINIA ELECTRONIC CASE FILING POLICIES AND PROCEDURES MANUAL, CHAPTER THREE: POLICIES AND PROCEDURES 23 (2013), http://www.vaed.uscourts.gov/ecf/documents/Chapter3-PoliciesandProcedureswithTitlePage1-11-16.pdf [https://perma.cc/KT8V-FP6Y] (creating exception to e-filing rules for warrant-type documents); *see also* U.S. DIST. COURT DIST. OF ARIZ., ELECTRONIC CASE FILING ADMINISTRATIVE POLICIES AND PROCEDURES MANUAL 23 (2016), http://www.azd.uscourts.gov/sites/default/files/documents/adm%20manual.pdf [https://perma.cc/RV7M-M2SX] (same); U.S. DIST. COURT FOR S. DIST. OF CAL., ELECTRONIC CASE FILING ADMINISTRATIVE POLICIES AND PROCEDURES MANUAL 19 (2017), https://www.casd.uscourts.gov/CMECF/Lists/Policies%20and%20Procedures/Attachments/8/CASDPolicies_01-20-2017.pdf [https://perma.cc/YVK5-7N7R] (same); U.S. DIST. COURT S. DIST. OF TEX., ADMINISTRATIVE PROCEDURES FOR ELECTRONIC FILING IN CIVIL AND CRIMINAL CASES 1 (2007), http://www.txs.uscourts.gov/sites/txs/files/admcvcrproc.pdf [https://perma.cc/5K78-KHET] (same); C.D. CAL. L. CR. R. 49-1.2 (same); D. D.C. CT. R. 49(e) (same).

113. Peter W. Martin, *Online Access to Court Records*, 53 VILL. L. REV. 855, 864 (2008).

114. *See, e.g.*, Lynn M. LoPucki, *The Politics of Research Access to Federal Court Data*, 80 TEX. L. REV. 2161, 2165 (2002) (writing that the U.S. Party/Case Index in an early version of PACER was "of marginal value for research because one can enter only a single name at a time and get only the name of the court and the number of the file").

115. *See, e.g.*, 18 U.S.C. § 3123(d) (2012) (requiring sealing "until otherwise ordered by the court"); *id.* at § 2705 (providing for delayed notice).

necessary, either renew or remove sealing requirements later in time. For example, the Eastern District of Missouri provides that applications for search warrants are "received by the Court under temporary seal," but that continued secrecy requires a motion "establishing a compelling interest necessitating a restriction on public access" within fourteen days.[116] Likewise, the Southern District of Alabama requires "[a] publicly filed motion and order citing only the statutory authority for sealing" for electronic surveillance orders, but it also provides that sealed documents are to be unsealed after 120 days.[117]

It is intuitive that, as a practical matter, sunset provisions that create an automatic, mandatory docket entry reminding the court that a docket, application, or order is due to be unsealed are likely to result in more unsealing than those that require action by the government or sua sponte by the court. Sunset provisions that mandate routine *unsealing* of search warrant returns and other sealed documents can greatly reduce the number of judicial documents that remain secret in the long term.

An ongoing case provides an illustrative example of the obstacles to gaining access to surveillance materials. Researchers in the Northern District of California have alleged that that district maintains an entirely sealed docket for applications and orders under the SCA and the Pen/Trap Statute.[118] The petitioners sought the docketing and unsealing of court records related to matters arising under the Wiretap Act, the SCA, and the Pen/Trap Statute.[119] In response, the federal government requested an opportunity to be heard because it "has an overarching interest in enforcing federal law, including these confidentiality provisions."[120] During oral argument on the petitioners' motion, the government notified the court that the United States Attorney's Office was "reviewing its own files to see what could be unsealed."[121] Months later, the government has still not unsealed a single item from the thousands of surveillance orders issued between 2006 and 2011 that the

116. E.D. MO. L.R. 83-13.05.

117. S.D. ALA. GEN. L.R 5.2.

118. Petition to Unseal Technical-Assistance Orders & Materials, *In re* Petition of Jennifer Granick & Riana Pfefferkorn to Unseal Tech.-Assistance Orders & Materials, No. 16-mc-80206-KAW (N.D. Cal. Sept. 28, 2016), ECF No. 1.

119. *Id.*

120. United States' Statement of Interest at 3, *In re Petition of Jennifer Granick*, No. 16-mc-80206-KAW (Oct. 13, 2016), ECF No. 6.

121. Order Denying Motion to Unseal Documents & Publicly Docket Court Records, *In re Petition of Jennifer Granick*, No. 16-mc-80206-KAW (June 23, 2017), ECF No. 36 [hereinafter Order Denying Motion].

prosecutors were reviewing.[122] And without a functioning public docket, petitioners cannot even identify—let alone move to unseal—individual cases of interest.[123]

Notwithstanding these flaws, the court concluded that, while a qualified right of access to electronic surveillance orders exists, it lacked the authority to "reverse the sealing orders of other judges in this district."[124] Moreover, the court determined that the petition was overbroad because some of the surveillance orders may pertain to investigations that were still active, and the petitioners had not identified particular cases that were closed and could be unsealed.[125] This finding flouts the traditional rule that the government bears the burden to justify closure, and ignores that the government's ability to do so may well erode over time.[126] Moreover, the court's position that its hands were tied with regard to other cognate courts' sealing orders ignores the systemic issues raised by the petitioners concerning the problematic docketing and sealing practices of the Northern District. The case is still ongoing.[127]

The result of this ad-hoc, patchwork system is that district courts around the country offer drastically different degrees of transparency and accessibility with regard to judicial documents related to surveillance. Even in districts where routine unsealing is the rule, local practices may make it difficult to identify and locate dockets that include electronic surveillance applications and orders. As a practical matter, the inconsistency among the districts makes it difficult for the public to understand either local or national patterns regarding electronic surveillance—for example, whether a certain U.S. Attorney's office seeks pen registers at a rate that is far below the norm, or whether a given judge does not require sealing orders in some types of cases. As a legal matter, local rules and practices that permit sealing of electronic

122. Joint Status Report at 1, *In re Petition of Jennifer Granick*, No. 16-mc-80206-KAW (Aug. 22, 2017), ECF No. 38 ("To date, no currently sealed criminal miscellaneous matters from that time period have been determined to be suitable for unsealing.").

123. *Id.* at 10 ("With little to no information available to us, how could Petitioners could [sic] even learn of the existence of 'particular historical matters' to which we might wish to seek access, much less ask the Court for access to them?").

124. Order Denying Motion, *supra* note 121.

125. *Id.*

126. *See* Globe Newspaper Co. v. Super. Ct. for Norfolk Cty., 457 U.S. 596, 606 (1982) ("[T]he State's justification in denying access must be a weighty one.").

127. *See* Order Continuing Status Conference, *In re Petition of Jennifer Granick*, No. 16-mc-80206-KAW (June 23, 2017), ECF No. 45 (continuing status conference until March 2018).

surveillance applications without either factual findings or provisions regarding unsealing violate the First Amendment and the common law.

### *C. Applying the Right of Access to Surveillance Records*

The near-automatic application of secrecy requirements under the Pen/Trap Statute and the SCA implicates two interrelated doctrinal questions: how the First Amendment right of access should apply to novel forms of proceedings, and whether the right attaches to documents that were issued ex parte. Today, dozens of federal statutes appear to require or authorize sealing of judicial documents as a rule, without any analysis or findings by the court.[128] These statutes, many of which were enacted in the fairly recent past, raise questions about whether the statutes impede access to documents to which the public has a constitutional right of access.

Courts have taken two main approaches to resolving whether the First Amendment right of access attaches to judicial records.[129] The first, "bifurcated" approach requires a litigant to establish both that the records to which she seeks access have historically been open and that transparency of those records serves a positive function.[130] The second, "complementary" approach finds that the right of access to documents attaches when it is a "necessary corollary of the capacity to attend the relevant proceedings."[131]

Applying the first approach, courts have disagreed about how strictly to enforce the historical prong of the First Amendment test, particularly with regard to new proceedings. Courts following the strict historical approach usually conclude that, without a lengthy tradition of access to the particular proceeding at issue, no First Amendment right attaches.[132] For example, in the only appellate decision considering whether the First

---

128. *See* Memorandum from Andrea Thomson to Dan Coquillette & Richard Marcus (Dec. 10, 2007) (on file with author).

129. *In re* New York Times Co. to Unseal Wiretap & Search Warrant Materials, 577 F.3d 401, 409 (2d Cir. 2009) ("We have previously endorsed two approaches to determine whether the First Amendment right of access extends to particular judicial records.").

130. United States v. Gonzales, 150 F.3d 1246, 1258 (10th Cir. 1998) (describing the reasoning, "adopted by some courts, that the *Press-Enterprise II* analysis requires *both* the experience and logic prongs to be satisfied" (emphasis in original)).

131. Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 93 (2d Cir. 2004); *see also* Doe v. Pub. Citizen, 749 F.3d 246, 267 (4th Cir. 2014) (recognizing Fourth Circuit's adoption of the *Pellegrino* approach).

132. *See In re* Boston Herald, Inc., 321 F.3d 174, 182 (1st Cir. 2003) (citing United States v. El-Sayegh, 131 F.3d 158, 160–61 (D.C. Cir. 1997); Baltimore Sun Co. v. Goetz, 886 F.2d 60, 64 (4th Cir. 1989)) (declining to decide whether to adopt the strict "two-prong" approach).

Amendment right of access attaches to SCA orders, the Fourth Circuit reasoned that because of the SCA's recent vintage, it could identify "no long tradition of access specifically for § 2703(d) orders," and the right of access therefore did not apply.[133] The D.C. Circuit has taken the same approach in noting that "[t]here can hardly be a historical tradition of access to the documents accompanying a procedure that did not exist" until established by judicial decision in 1991.[134]

Courts that adhere to a strict historical approach ignore the serious costs of allowing Congress to require secrecy in everyday judicial proceedings. These rulings tacitly permit Congress to displace the right of access merely by creating new, secret procedures—an endeavor that raises concerns not only about constitutional rights, but also about the separation of powers.[135] This rigid approach also tends to ignore that—as Judith Resnik has pointed out in the context of alternative dispute resolution and arbitration—as statutory and technological change "reshape 'experiences,' they alter the 'logic' of what courts are about and when openness is therefore protected."[136]

Other courts have found that it is appropriate to "de-emphasize historical practices" if the proceeding or document in question is novel.[137] This variation of the bifurcated approach has been particularly developed in the context of criminal pretrial proceedings such as suppression hearings, which "have no historical counterpart."[138] Courts adopting this approach have recognized that, at the time of the framing, "no one could have conceived that the exclusionary rule and pretrial motions to suppress evidence would be part of our criminal jurisprudence."[139] Appellate courts have concluded that searching for

---

133. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 291 (4th Cir. 2013).

134. United States v. El-Sayegh, 131 F.3d 158, 161 (D.C. Cir. 1997).

135. *See infra* section II.A.

136. Judith Resnik, *The Privatization of Process: Requiem for and Celebration of the Federal Rules of Civil Procedure at 75*, 162 U. PA. L. REV. 1793, 1816 (2014).

137. Minneapolis Star & Tribune Co. v. Kammeyer, 341 N.W.2d 550, 556 (Minn. 1983) (First Amendment right of access attaches to pretrial hearing on motions to suppress and to change venue); *see also In re* Copley Press, Inc., 518 F.3d 1022, 1026 (9th Cir. 2008) ("[L]ogic alone, even without experience, may be enough to establish the right.").

138. *Press-Enterprise II*, 478 U.S. 1, 10 n.3 (1986).

139. Richmond Newspapers, Inc. v. Commonwealth, 281 S.E.2d 915, 922 (Va. 1981) (quoting Gannett Co. v. DePasquale, 443 U.S. 368, 395–96 (Burger, C.J., concurring)); *see also* United States v. Criden, 675 F.2d 550, 555 (3d Cir. 1982) ("We do not think that historical analysis is relevant in determining whether there is a first amendment right of access to pretrial criminal proceedings."); Iowa Freedom of Info. Council v. Wifvat, 328 N.W.2d 920, 923 (Iowa 1983) (suppression hearings "are creatures unknown to traditional common law").

historical patterns of access to pretrial hearings is often in vain: "[t]he most one could do is search for some pattern of access or non-access which may have developed in the area," but such a pattern may not exist.[140] Indeed, in some areas, a presumption of openness has developed even in the absence of "centuries of tradition."[141] In light of the fact that many pretrial hearings simply did not exist at common law, "the lack of an historic tradition of open . . . hearings does not bar our recognizing a right of access to such hearings."[142]

To complicate matters further, some courts have adopted an alternative method of applying the right of access to judicial records, recognizing that the right of access to documents is a "necessary corollary of the capacity to attend the relevant proceedings."[143] Rather than asking whether there is a history and logic to openness of the records themselves, this "complementary" approach asks whether the documents are tied to a judicial proceeding which the public has a constitutional right to attend.

But proceedings for the issuance of the orders are historically ex parte.[144] Although warrant affidavits and returns are typically filed with the clerk after a search is executed, courts have concluded that that practice is "not demanded by the [F]irst [A]mendment."[145] Moreover, it certainly remains true that pretrial proceedings for the issuance of search warrants or surveillance orders are "necessarily *ex parte*, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence."[146]

Courts that follow the "necessary corollary" approach would likely reject a right of access to surveillance and warrant materials because

---

140. United States v. Gonzales, 150 F.3d 1246, 1257 (10th Cir. 1998).

141. Buzbee v. Journal Newspapers, Inc., 465 A.2d 426, 431 (Md. 1983).

142. United States v. Chagra, 701 F.2d 354, 363–64 (5th Cir. 1983) (quoting *Gannett*, 443 U.S. at 401 (Powell, J., concurring)) (holding that a First Amendment right of access attaches to bail reduction hearings, but that the right "extends no farther than the persons actually present at the time the motion [for bail] is made"); *see also* Seattle Times Co. v. D. for the W.D. of Wash., 845 F.2d 1513, 1516 (9th Cir. 1988) (finding a First Amendment right of access to pretrial release proceedings).

143. Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 93 (2d Cir. 2004); *see also* Doe v. Pub. Citizen, 749 F.3d 246, 267 (4th Cir. 2014) (recognizing Fourth Circuit's adoption of the *Pellegrino* approach).

144. *See* Baltimore Sun Co. v. Goetz, 886 F.2d 60, 64 (4th Cir. 1989) (citing Franks v. Delaware, 438 U.S. 154, 169 (1978)).

145. *Id.*

146. *Franks*, 438 U.S. at 169 (quoted in *In re* The Search of Fair Fin., 692 F.3d 424, 430 (6th Cir. 2012)).

there is no contemporaneous right of access to the underlying ex parte proceedings in which they are issued. In 2012, the Sixth Circuit relied on the ex parte nature of warrant proceedings to reject an attempt by two news organizations to gain access to search warrant materials filed under seal.[147] The newspapers argued that under Rule 41, the obligation to deliver the executed warrant to the clerk is suggestive of a historical practice of openness, as "once the search warrant documents are returned to the clerk, they are routinely filed without seal."[148] The court, however, found it "indisputable that proceedings for the issuance of search warrants are not, and have not been, public."[149]

Nevertheless, as Lynn Oberlander points out, several circuits have extended the *Press-Enterprise II* holding to search warrant affidavits, with mixed results.[150] For example, in 1989 the Ninth Circuit held that "members of the public have no right of access to search warrant affidavits while a pre-indictment investigation is under way."[151] The same year, the Fourth Circuit likewise rejected the Baltimore Sun's assertion of a "right of access to inspect and copy affidavits supporting search warrants in the interval between execution of the warrants and indictment."[152] Neither court considered whether a right of access may attach *after* indictment or the resolution of an investigation.[153] The Eighth Circuit has concluded that the public has a First Amendment right of access to search warrant affidavits even before an indictment had issued.[154] The disparate outcomes of applications for access to

147. *In re The Search of Fair Fin.*, 692 F.3d at 428. The news organizations filed a pre-indictment motion for access to the search warrant materials, but by the time the court of appeals ruled on the issue, an indictment had been issued. The court of appeals did not address the effect of this procedural change, if any, upon the attachment of the First Amendment right.

148. *Id.* at 430.

149. *Id.* Although the court of appeals disagreed, the opinion also "reject[ed] the government's suggestion that there is no First Amendment right of access to the search warrant documents here due to the fact that the search warrant application process is an investigative rather than a criminal proceeding." *Id.*

150. *See* Lynn B. Oberlander, *A First Amendment Right of Access to Affidavits in Support of Search Warrants*, 90 COLUM. L. REV. 2216, 2217 (1990).

151. Times Mirror Co. v. United States, 873 F.2d 1210, 1211 (9th Cir. 1989).

152. Baltimore Sun Co. v. Goetz, 886 F.2d 60, 62 (4th Cir. 1989).

153. *See also In re* EyeCare Physicians of Am., 100 F.3d 514, 516 (7th Cir. 1996) (rejecting EyeCare's due process argument that it was entitled to the affidavits in support of the search warrant executed on its property, "for no person affiliated with EyeCare has even been indicted, much less deprived of life or liberty").

154. *In re* Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d 569, 575 (8th Cir. 1988).

search warrant materials appear to depend at least partly on the status of the investigation at the time of the request.[155]

Only the Fourth Circuit has explicitly considered whether a right of access attaches to orders issued under the SCA.[156] In *In re Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(d)*,[157] the Fourth Circuit was presented with an order and application relevant to the "pre-grand jury phase of an ongoing criminal investigation."[158] As the district court in that case observed, "there is no history of openness for documents related to an ongoing criminal investigation."[159] As a result, the Fourth Circuit summarily concluded that § 2703(d) orders "are most analogous to sealed or unexecuted search warrants and grand jury proceedings for which traditionally, there is no history of access."[160]

## II. A HISTORY OF PUBLIC SEARCHES

Even if the public has no right to attend proceedings at which search warrants and surveillance orders are issued, public access to the related materials might be a "necessary corollary" of a different proceeding: the search itself. There is a rich and unexplored history of open access to searches and seizures. During the framing generation and thereafter, public *observation* of searches and seizures, in real time and space as

155. *See In re* The Search of Fair Fin., 692 F.3d 424 (6th Cir. 2012) (no First Amendment right of access); *In re EyeCare Physicians of Am.*, 100 F.3d at 517 (holding that no right of access to search warrant materials attaches under the Fourth Amendment); *In re* Application of Newsday, Inc., 895 F.2d 74, 78 (2d Cir. 1990) (avoiding the constitutional question by finding a common law right attaches); *Goetz*, 886 F.2d at 65 (finding that, while no right of access to search warrant materials attaches under the First Amendment, notice was still required); *Times Mirror Co.*, 873 F.2d at 1216 ("[T]he First Amendment does not establish a qualified right of access to search warrant proceedings and materials while a pre-indictment investigation is still ongoing.").

156. *See In re* Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 291–92 (4th Cir. 2013) (concluding that no First Amendment right of access attaches to SCA orders); *see also* Craig Linder, *Dow Jones Fights for Transparency*, DOW JONES (June 3, 2014), http://www.dowjones.com/press-room/dow-jones-fights-transparency/ [https://perma.cc/J2GJ-UX44] (finding that no First Amendment right attaches, and common law does not require access).

157. 707 F.3d 283 (4th Cir. 2013).

158. *Id.* at 286.

159. *In re* § 2703(d) Order, 787 F. Supp. 2d 430, 443 (E.D. Va. 2011).

160. *In re Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d at 292 n.9. *But see In re* Leopold to Unseal Certain Elec. Surveillance Applications & Orders, No. 13-MC-00712, 2018 WL 1129660, at *14 (D.D.C. Feb. 26, 2018) ("[N]one of the materials to which the petitioners seek access—not even SCA warrants—are analogous to traditional search warrants.").

well as in the press, fostered criticism, debate, and resistance to abuses of power that were then proscribed in the Fourth Amendment.

The Fourth Amendment grew out of a general consensus in the Framing generation against general, warrantless, and abusive searches of homes and private places.[161] The two clauses of the Amendment—the first ensuring the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," the second proscribing the issuance of warrants except "upon probable cause, supported by oath or affirmation, and *particularly describing the place to be searched*, and the persons or things to be seized"—evinced the Framers' reaction to two types of abuses suffered for centuries under British rule.[162]

A full accounting of the contested history and historiography of the framing of the Fourth Amendment is far beyond the scope of this Article.[163] Indeed, the hotly disputed questions surrounding the framing of the Fourth Amendment—the relationship between the two clauses of the Amendment, the historical understanding of the terms "unreasonable" and "probable cause," and the Framers' intentions regarding the scope of the Amendment—only tangentially abut this Article's main claims. Instead, this Part demonstrates that, far from being insulated from public view, searches and seizures were quintessentially public proceedings, and their very openness laid bare abuses of power that required democratic oversight. It was the invention of warrantless policing, in lockstep with technological change, that facilitated secrecy.

---

161. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 70.

162. U.S. CONST. amend. IV (emphasis added).

163. *See generally* WILLIAM CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING lxvi (2009) ("Many kinds of searches and seizures were unreasonable within the original meaning of the amendment, not just general warrants."); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994) (arguing, generally, that the Fourth Amendment was intended to require reasonableness, not warrants); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 398 (1974) (arguing that the effort to reconstruct Fourth Amendment history is "illusory"); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 551 (2000) ("[T]he Framers did not address warrantless intrusions at all in the Fourth Amendment or in the earlier state provisions; thus, they never anticipated that 'unreasonable' might be read as a standard for warrantless intrusions."); Tracey Maclin & Julia Mirabella, *Framing the Fourth*, 109 MICH. L. REV. 1049 (2011) (placing Cuddihy's contribution in the context of scholarly debates between Amar, Davies, and others); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 825 (1994) ("[I]t is perfectly appropriate for twentieth-century judges to forge a new connection between reasonableness and warrants and to create a new constitutional remedy in light of our post-colonial history.").

### *A. Searches as "Public Spectacle"*

When the Framers demanded that searches be reasonable and that warrants be limited in scope, they were responding to the common law legacy of unfettered power of discretionary searches.[164] These concerns were tangible: the "harsh experience of householders having their doors hammered open by magistrates and writ-bearing agents of the crown" gave rise to the principles set forth in the Fourth Amendment that limited the government's ability to search.[165] The "sacrosanct interest" in privacy in the home required heightened protections from searches.[166] A vivid 1788 commentary called on readers to "imagine the dreadful giant Congress storming our domestic castles by warrants both general and special, and searching our cellars, garrets, bed-chambers and closets," admonishing them not to be "such gentle doves as to let any cormorants rifle your nests, snatch the victuals from your little ones, and tear the covers from your beloved mates."[167] "Open your front door, ran the argument, and the extent of federal invasion will be infinite. Kitchens and closets, cellars and garrets, bedchambers and trunks, desks and letters, petticoats, and pockets: none will remain inviolate to scrutiny."[168]

The 1766 "Malcom affair," which one scholar has called "the most famous search in colonial America," exemplified the type of domestic intrusion that the Framers wished to prevent.[169] On the authority of a writ of assistance issued a year prior, two customs officers entered Malcom's house to search for smuggled brandy and liquor. Despite claiming innocence, Malcom "opened every place in his house that his visitors wished to see, including his wood shed and two cellars."[170] When Malcom refused the officers' demand that Malcom open a third cellar compartment, the customs officers called in reinforcements to break in: Malcom then armed himself with pistols and a sword and threatened to kill the searchers.[171] The searchers left, then returned with

---

164. Davies, *supra* note 163, at 578 ("Common-law authorities repeatedly gave a consistent reason for condemning general warrants: if such warrants had been permitted, they would have conferred on ordinary officers discretionary authority to arrest or even to search houses.").

165. William Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 371, 372 (1980).

166. Davies, *supra* note 163, at 642.

167. CUDDIHY, *supra* note 163, at 679.

168. *Id.* at 766.

169. *Id.* at 496.

170. *Id.* at 497.

171. *Id.*

a specific search warrant, only to find that Malcom had fortified his house, locking "every window, door, and gate."[172] The customs officers began calling upon bystanders to help them break in, but to no avail.[173] "Many in the crowd sympathized with Malcom and angrily refused to help; others were willing to assist only after he had been subdued."[174]

The Malcom affair also illustrates another critical aspect of searches in the colonial era: they occurred in public, in real time and space. Indeed, it was precisely the public nature of the Malcom search, the sight of the customs officers bellowing at Malcom's home-turned-castle, that attracted scrutiny and resistance from passersby who refused to help. Likewise, legislators in the colonial era were hostile to other measures that would tend to expedite searches and insulate them from public view, repudiating nocturnal searches and no-knock entry.[175] These limitations on the power to search ensured not only that individuals were protected from unlawful, abusive searches, but also that searches were executed in daylight, perhaps with neighbors and curious bystanders watching. The very public nature of searches and seizures, coupled with the abusive practice of general and discretionary searches, fostered the population's distrust, antipathy, and ultimately obstruction of colonial officers who undertook them: "[t]arred and feathered customs officers, cowed magistrates, and mob 'liberations' of seizures flooded newspapers and correspondence."[176]

Searches were transparent in another way: after a search was completed and property seized, an inventory was required to be left with the individual searched.[177] In the seminal case of *Wilkes v. Wood*,[178] a dissenting printer filed an action for trespass after the government searched and seized all of his papers; a chief objection to the unreasonableness of the blanket search was that the searchers had failed

172. *Id.* at 498.

173. *Id.*

174. *Id.* at 499. In the wake of the Malcom affair, Sir Francis Bernard, Governor of Massachusetts, sent depositions to England to "remind Westminster yet again of Boston's incorrigible turbulence"—and to prompt Parliament to enact statutory permission for writs of assistance searches in the colonies. M.H. SMITH, THE WRITS OF ASSISTANCE CASE 447–54 (1978).

175. CUDDIHY, *supra* note 163, at 660–61.

176. *Id.* at 511.

177. *In re* Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d 569, 573 (8th Cir. 1988) ("[A]lthough the process of issuing search warrants has traditionally not been conducted in an open fashion, search warrant applications and receipts are routinely filed with the clerk of court without seal."). This requirement is mirrored in Federal Rule of Criminal Procedure 41.

178. (1763) 98 Eng. Rep. 489.

to leave an inventory behind.[179] At a minimum, the logic ran, the government had to inform the target of a search and seizure of what had been taken. During the founding era, however, executed warrants were "retained by the constable," not filed with a central clerk's office for all to see.[180]

The law of search and seizure was also itself made public: William Cuddihy reports that, in the wake of the revolution, "practically all" legislation restricting searches and seizures was published, making the "major developments in search and seizure readily accessible."[181] Yet these publications provoked scant response from the public, a fact that Cuddihy attributes, in part, to the traumatic effects of plunder during the war: "[w]hen heavily armed men kicked in the door in the dead of night and demanded to be fed, the persons behind that door reacted with terror and outrage, not with arguments for specific search warrants or evaluations of probable cause."[182]

Given this background, it is perhaps unsurprising that the framers of the Fourth Amendment retained a deeply physical, place-based conception of what ought to be protected from the unfettered, general power to search homes and seize property. In order to prevent law enforcement from using general warrants, the framers chose to require a warrant to specify the "place" to be searched.[183] Spatial limits were integral to the Fourth Amendment's restrictions on the power to search and seize.

Yet the framing generation also recognized that physical searches implicated ephemeral ideas. In crying out for protection from unfettered home searches, commentators "expressed concern for 'the most delicate parts of our families,' for 'most discreet recesses,' 'private papers,' and 'private concerns,' in short, for privacy."[184] The special protections from

---

179. *Id.* at 498 ("The defendants claimed a right, under precedents, to force persons houses, break open escrutores, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall.").

180. Davies, *supra* note 163, at 642 n.257.

181. CUDDIHY, *supra* note 163, at 666.

182. *Id.* at 667.

183. U.S. CONST. amend. IV. Cuddihy observes that the contemporary definition of "place" was a "particular portion of space," concluding that by limiting warrants to one "place," Congress intended to "restrict the resulting search not only to a single building, but, if possible, to a segment of it or to a unique area of space, even if it did not constitute a fully enclosed structure." CUDDIHY, *supra* note 163, at 742.

184. *Id.* at 766; *see also* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 397 (2008) (quoting Justice Brandeis's dissenting opinion in Olmstead v. United States, 277 U.S. 438, 478

search that the Framers conferred upon "papers" also emanated partly from the English history of using search and seizure to control religious and political dissent.[185] William Stuntz also emphasizes the historical salience of the seditious libel cases of *Entick v. Carrington*[186] and *Wilkes*, two "classic First Amendment cases in a system with no First Amendment."[187] In short, the Fourth Amendment was rooted in the public backlash to abusive, discretionary *physical* searches of homes and private places, but was equally intended to protect against invasion of the intangible interests of privacy and expressive and religious freedom as against physical intrusions.

### *B. Secrecy, Compulsion, and Coercion Under the Fourth Amendment*

The presumption that searches were public, and publicly accountable, continued into the nineteenth century. Most early Fourth Amendment cases continued to involve open, physical searches, not secret ones. As a result, the early doctrine tended to emphasize how the government's use of force and compulsion—factors that were tangible to those who were searched—rendered home searches unreasonable. For example, in *Boyd v. United States*,[188] the Court distinguished between the "search and seizure of a man's private papers, or the compulsory production of them, for the purpose of using them in evidence against him in a criminal case," and the search and seizure of goods that were contraband.[189] The *Boyd* Court did not contemplate a secret search, but a compelled disclosure of papers; accordingly, it found that "any *forcible* and *compulsory* extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods," is prohibited by the Constitution.[190]

In two later cases, the Court rejected secret, warrantless searches, even when they involved no outright force or overt compulsion. In 1914,

---

(1928) (the Framers "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations")).

185. CUDDIHY, *supra* note 163, at 55–60 (detailing how English monarchs targeted "seditious" and "heretical" religious books and manuscripts for searches and seizures after the Reformation and the Restoration and well into the mid-seventeenth century).

186. (1765) 95 Eng. Rep. 807; 19 Howell's State Trials 1029.

187. William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 403 (1995). *But see* Davies, *supra* note 163, at 573 n.57 (claiming that Stuntz erred in concluding that search warrants at the framing were rare).

188. 116 U.S. 616 (1886).

189. *Id.* at 623.

190. *Id.* at 630 (emphasis added).

the Court considered in *Weeks v. United States*[191] a physical search of a suspect's home while he was absent.[192] The defendant had been arrested at the train station where he worked. While he was under arrest, the police went to his house, located—with a neighbor's assistance—the spare key, and let themselves in to seize some of his books and papers.[193] Later that day, the police returned with the marshal; a neighbor let them in and they searched again.[194] The defendant petitioned for the return of his property, and the Court refused to sanction the search, holding, by implication, that a court has no authority "to retain for the purposes of evidence the letters and correspondence of the accused, seized in his house *in his absence and without his authority*, by a United States Marshal holding no warrant for his arrest and none for the search of his premises."[195]

In *Gouled v. United States*,[196] the Supreme Court explicitly recognized that "the *secret* taking or abstraction, without force, . . . of a paper writing of evidential value only belonging to one suspected of a crime and from the house or office of such a person" constituted a Fourth Amendment "search."[197] *Gouled* involved a conspiracy to defraud the United States through contracts for the provision of clothing and equipment.[198] Suspicious of dishonest conduct, the "Intelligence Department" of the U.S. Army asked Cohen, who was both a private in the Department and a business acquaintance of Gouled's, to investigate.[199] Pretending to pay a "friendly call," Cohen stole several documents from Gouled's office in his absence.[200] Six months later, agents of the Department of Justice secured warrants permitting them to search Gouled's office for "letters, papers, documents, and writings" relating to the conspiracy.[201] Gouled was aware of the warrants, but

191. 232 U.S. 383 (1914), *overruled on other grounds by* Mapp v. Ohio, 367 U.S. 643 (1961).

192. *Id.* at 386.

193. *Id.*

194. *Id.*

195. *Id.* at 393 (emphasis added). *Silverthorne Lumber Co. v. United States* also presented a situation in which the defendants' office was searched in their absence and without a warrant while they were detained in custody, and the Court once again rebuked the government. 251 U.S. 385 (1920).

196. 255 U.S. 298 (1921).

197. *Id.* at 305, *abrogated by* Warden v. Hayden, 387 U.S. 294 (1967) (emphasis added).

198. *Id.* at 304.

199. Gouled v. United States, 264 F. 839, 839 (2d Cir. 1920).

200. *Id.* at 839.

201. *Id.* at 840.

according to the Second Circuit, which certified the question to the Supreme Court, "Gouled did not know what Cohen had done" until Cohen testified before the grand jury.[202]

Once again, the Court rejected the notion that "[e]ither actual force or legal compulsion" were necessary ingredients for an unconstitutional search.[203] Recognizing that forcible entry would render a resulting search unreasonable, the Court reasoned that "it is impossible to successfully contend that a like search and seizure would be a reasonable one if only admission were obtained by stealth instead of by force or coercion."[204] The owner's "security and privacy" would be "as much invaded" in both cases, the Court found, and held that whether law enforcement enters a home or office "by stealth, or through social acquaintance, or in the guise of a business call, and whether the owner be present or not when he enters, any search and seizure subsequently and secretly made in his absence" is proscribed by the Fourth Amendment.[205]

### *C. Eavesdropping and Wiretapping*

The development of wiretapping and eavesdropping weakened the Court's resolve that secret searches were equally off-limits as forcible ones. In 1928, the *Olmstead* Court held that eavesdropping on telephone conversations, without a physical trespass, implicated no Fourth Amendment rights. Recharacterizing the "stealthy entrance" in *Gouled* as "the equivalent to an entry by force," the Court rejected the idea that the Fourth Amendment could also be violated in intangible ways, dismissing the eavesdropping as representative "only of voluntary conversations secretly overheard."[206] The *Gouled* decision, the Court said, represented the "extreme limit" of the Fourth Amendment.[207]

In dissent, Justice Brandeis recognized that new technology made secret searches as easy to accomplish as those achieved by force or compulsion. Just so, Justice Brandeis argued that the government's possession of "[s]ubtler and more far-reaching means" of searching and

---

202. *Id.*

203. *Gouled*, 255 U.S. at 299.

204. *Id.* at 305.

205. *Id.* at 306.

206. Olmstead v. United States, 277 U.S. 438, 463–64 (1928). The Court appeared to shy away from the "sweeping" results of *Weeks* and its progeny, which had resulted in the outright exclusion of evidence from criminal proceedings rather than the imposition of *ex post* liability. *Id.* at 463.

207. *Id.*

seizing made the Court's focus on tangible harms irrelevant; government agents need no longer resort to "stretching upon the rack."[208]

Nor did Justice Brandeis accept the Court's assertion that only visible, tangible searches warranted constitutional protections, instead quoting the dissenting opinion from the Ninth Circuit: "[t]rue the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference."[209]

Following *Olmstead*, Congress recognized that even warrantless, secret, and—in some sense—intangible surveillance of conversations implicated civil liberties. In the Federal Communications Act of 1934, Congress prohibited law enforcement from wiretapping conversations.[210] But that statutory prohibition was frequently ignored; indeed, the Department of Justice interpreted the Act to permit interception, "so long as no disclosure of the content outside the Department is made."[211] From 1928 until 1967, in other words, no warrant or judicial order was required for electronic surveillance. As a result, during that period law enforcement operated in the dark, almost entirely without oversight by the courts or the public.[212]

### *D. "Necessarily Secret" Electronic Searches Emerge*

In the 1960s, the Court began once again to shift its approach to the constitutional problems raised by secret, warrantless communications surveillance. In *Berger*, the Court found fault with the New York eavesdropping statute's failure to provide for notice to the target of a wiretap, even as the majority conceded that the statute's "success depends on secrecy."[213] Subsequently, the Court overtly repudiated the "trespass-based" theory of the Fourth Amendment in its 1967 ruling in *Katz v. United States*[214] and held that electronic surveillance, in the absence of physical trespass, still constituted a "search."[215]

---

208. *Id.* at 473 (Brandeis, J., dissenting).

209. *Id.* at 475.

210. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 26 (2004).

211. Berger v. New York, 388 U.S. 41, 127 (1967) (White, J., dissenting).

212. Freiwald, *supra* note 210, at 26.

213. *Berger*, 388 U.S. at 60. In dissent, Justice Black lambasted the majority's "notice" requirement as a "fantastic suggestion" that was fundamentally at odds with the fact that "secrecy is an essential, indeed a definitional, element of eavesdropping." *Id.* at 86 (Black, J., dissenting).

214. 389 U.S. 347 (1967).

215. *Id.* at 353.

In recognizing that the Fourth Amendment attaches to telephonic communications, the Court nonetheless distinguished eavesdropping from physical searches, finding that judicially "authorized electronic surveillance" required no prior notice.[216] The Court rejected the Fourth Amendment's "knock and announce" requirement as inapplicable to eavesdropping, just as "officers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence."[217] *Katz* ushered in a new era of judicially sanctioned secret searches that had previously been unregulated, bringing wiretapping and electronic surveillance under the supervision of magistrates.

In response to *Katz* and *Berger*, Congress enacted the Wiretap Act in 1968. The Act "[w]ork[ed] from the hypothesis that any wiretapping and electronic surveillance legislation" should respond to the concerns raised in *Katz* and *Berger*, including the requirement of notice to targets.[218] The Department of Justice recognized that *Berger* and *Katz* "established that notice *must* be served on *all* parties to intercepted communications,"[219] but that prior notice was impracticable in the electronic surveillance context. Because ex post notice was likewise required under "existing search warrant practice[s]," Congress substituted a requirement that law enforcement serve an inventory on the target of a wiretap *after* the interception.[220] Conceding that, under certain circumstances, the government might be able to postpone notice "almost indefinitely," the Senate nonetheless embraced the principle that subjects of surveillance would be informed, after the fact, that their communications had been intercepted.[221] This "principle of postuse notice," the Senate noted, not only guaranteed that surveillance "must eventually become known at least to the subject," but also performed an important public oversight function to "insure the community that the techniques are reasonably employed."[222]

The Wiretap Act also, however, codified a presumption of secrecy. This requirement stemmed from the same reasons eavesdropping warranted careful judicial oversight: it was intrusive. The Act set out

---

216. *Id.* at 355 n.16 (1967).

217. *Id.*

218. S. REP. NO. 1097, at 2163 (1968).

219. 114 CONG. REC. 6214 (May 23, 1968) (emphasis in original).

220. S. REP. NO. 1097, at 2194.

221. *Id.*

222. *Id.*

explicit requirements for applications to intercept communications and provided that applications made, orders granted, and recordings authorized under the act "shall be sealed by the judge" and disclosed "only upon a showing of good cause."[223]

While *Katz* expanded the coverage of the Fourth Amendment, the Court simultaneously broadened law enforcement's power to search by dismantling the "mere evidence" rule, which had historically limited law enforcement's ability to search for evidence unless it constituted an instrumentality, fruit of crime, or contraband.[224] In *Warden v. Hayden*,[225] only six months prior to *Katz*, the Court had repudiated that longstanding distinction, upholding the admission of a defendant's "cap, jacket, and trousers" as evidence in his trial for robbery.[226] This rejection of the "mere evidence" rule laid the groundwork for police to search for evidence of crime, even when it is "in the private files of a person not suspected of involvement in any criminal activity."[227]

Subsequently, the Court adopted the rule that an individual can have "no legitimate expectation of privacy in information he voluntarily turns over to third parties."[228] In 1976, the Court held in *United States v. Miller*[229] that a bank customer had no expectation of privacy, and thus no Fourth Amendment protection, regarding depositor records held by his bank.[230] The defendant in *Miller* not only lacked a legal right to challenge a subpoena issued to a third party, but also was not entitled to *notice* of that subpoena. In dissent, Justice Brennan characterized this lack of notice as a "fatal constitutional defect."[231]

The implications for telephone records were immediate. Two years after *Miller*, the D.C. Circuit held that reporters were not entitled to

---

223. 18 U.S.C. § 2518 (1968); *see also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801, 82 Stat. 211 (2013) ("To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.").

224. Warden v. Hayden, 387 U.S. 294, 300 (1967).

225. 387 U.S. 294 (1967).

226. *Id.* at 296.

227. Zurcher v. Stanford Daily, 436 U.S. 547, 577 (Stevens, J., dissenting).

228. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)).

229. 425 U.S. 435 (1976).

230. *Id.* at 442–43.

231. *Id.* at 448 n.2 (Brennan, J., dissenting); *see also* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) (precedent "disable[s] respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers").

notice before subpoenas were issued for telephone records reflecting communications with sources.[232] The following year, the Supreme Court held in *Smith v. Maryland*[233] that no search warrant was required for pen registers because, regardless of whether the petitioner wished to keep the "*contents*" of his conversations private, he had no expectation of privacy in the phone numbers he dialed.[234]

Taken together, *Katz*, *Hayden*, and the third-party doctrine substantially altered the constitutional protections against unfettered law enforcement access to telecommunications records. *Katz* made it possible for law enforcement to obtain search warrants in order to listen in on conversations. *Hayden* legitimized the use of searches that targeted even those not suspected of committing a crime. And *Smith* and *Miller* made plain that targets were not entitled to notice of the electronic surveillance that was occurring. None of these cases took account of the important functions that notice performed by keeping the government accountable in criminal investigations, both to defendants and to the public.

### *E. Statutory Secrecy Provisions in the Third-Party Context*

In 1986, when Congress enacted the Electronic Communications Privacy Act (ECPA), it reformed Title III and regulated the new kinds of electronic surveillance occurring under the third-party doctrine. While the Wiretap Act regulated real-time acquisition of communications content, the Pen/Trap Statute regulated real-time acquisition of communications metadata using pen registers, trap and trace devices, and tracking devices.[235] As the name suggests, the SCA regulated government acquisition of communications in storage, including both content and metadata.[236] All three authorities set out frameworks for the government to apply for court orders authorizing the acquisition of electronic communications information from service providers.

Like the Wiretap Act, the Pen/Trap Statute codified secrecy requirements, albeit with unclear congressional motivations. The 1985

---

232. Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1044 (D.C. Cir. 1978) ("[A] person has no Fourth Amendment basis for challenging subpoenas directed at the business records of a third party, and, hence, has no right to notice of such subpoenas.").

233. 442 U.S. 735 (1979).

234. *Id.* at 743–44 (emphasis in original).

235. The USA PATRIOT Act amended the Pen/Trap Statute to clarify that the government could use this authority to collect "dialing, routing, addressing, or signaling information" of "electronic communication[s]." *See* Susan Freiwald, *supra* note 210, at 49.

236. 18 U.S.C. § 2703 (2012).

versions of the bill from the House and the Senate were silent on judicial sealing requirements and provided that "the person owning or leasing the line" affected by the pen register may be able to disclose the existence of the order "60 days after its removal."[237] In addition, the Act provided that the judge who issued the order should notify the affected person within ninety days after the termination of a pen register.[238] In the final version, however, these provisions were absent; instead, Congress required that an order be sealed and the recipient gagged "until otherwise ordered by the court."[239]

At the same time that Congress adopted these secrecy requirements for electronic searches, the Fourth Amendment presumption against secret *physical* searches remained intact.[240] Even when the government executed "sneak and peek" warrants, which permit agents to enter a premises to gather information without leaving notice or an inventory, it was required to give advance or contemporaneous notice to the target of the search unless it demonstrates "reasonable necessity for the delay."[241] Even if notice might be delayed, sneak and peek warrants required "notice of the search within a reasonable time after the covert entry."[242] These safeguards were necessary because, as the Ninth Circuit put it, "surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment."[243]

In contrast, by substituting gag orders for notice requirements in the electronic context, Congress created a norm of secrecy without historical precedent. Although, as the Court recognized in *Berger* and *Katz*, electronic surveillance did not require prior or contemporaneous notice, ex post notice was still required. And in enacting the Wiretap Act, Congress recognized that "postuse notice" performed not only essential due process functions, but also served to keep the government accountable to the public. By contrast, the enactment of the Pen/Trap Statute included neither provisions for notice to targets nor for public accountability. The result was that the new third-party ecosystem

237. H.R. 3378, 90th Cong. § 3123 (1985).

238. *Id.*

239. 18 U.S.C. § 3123(d) (2010).

240. John Kent Walker, Jr., *Covert Searches*, 39 STAN. L. REV. 545, 554 (1987) (arguing that the extension of the warrant requirement to electronic surveillance represented a shift toward protection of privacy from protection of property).

241. United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).

242. *Id.*

243. United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986).

dramatically departed from the longstanding historical tradition of open, publicly accountable searches and seizures.[244]

### *F. First Amendment Implications of Fourth Amendment History*

This Fourth Amendment story has deep implications for how we understand the historical inquiry through the prism of the First Amendment right of access. The First Amendment requires courts to dive deep to understand whether a certain type of document or proceeding was historically open. But the historical experience of openness for search warrants, and the recognition of the importance of transparency and notice in the electronic surveillance context, suggest several different appropriate avenues for inquiry.

First, the experience of open, public searches at common law and long thereafter might suggest that searches and seizures are themselves "government proceedings" subject to a First Amendment right of access. Courts have recognized a historical tradition of public access to government proceedings that are "open to all comers" or are "fully open events."[245] The broad experience of public oversight, observation, and participation in searches and seizures strongly suggests that there is a long tradition of openness. Indeed, to the extent the Supreme Court addressed secret searches at all, it appeared to find them constitutionally dubious—that is, until technological change created a need for secrecy by facilitating eavesdropping, wiretapping, and other electronic surveillance.

Second, a history of closure that results from a *statutory* bar on openness does not, in and of itself, suggest that closure is either normatively desirable or constitutional. The fact that a statute permits or requires closure does not necessarily reflect a congressional belief that closure is either "consistent with historical practice or a significant departure."[246] As a result, the Tenth Circuit has suggested that looking to a history of closure that results from a statutory authorization of secrecy

244. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 802–03 (1994) (contrasting secret electronic surveillance, without notice, with physical warrants that "would be served on the owner or occupant of the searched premises, or left there, giving the target clear notice of what had been searched or seized, and when").

245. Cal. First Amendment Coal. v. Woodford, 299 F.3d 868, 875 (9th Cir. 2002) (characterizing executions as historically open).

246. United States v. Wecht, 537 F.3d 222, 237 (3d Cir. 2008).

is "obviously not required (and perhaps entirely inappropriate) as part of the 'experience' factor of *Press-Enterprise II*."[247]

It follows that courts ought to scrutinize the statutory sealing and secrecy requirements in the Pen/Trap Statute and the SCA, which purport to justify secrecy where it appears that in fact none was intended or required. The Supreme Court had recognized, in *Berger* and *Katz*, that while electronic searches necessarily had to take place in secret, ex post notice was an essential element of preventing government abuses. Likewise, in enacting the Wiretap Act, Congress had found that "postuse notice" served to keep the public informed of government activity. Against this background, the enactment of broad secrecy provisions in 1986 appears historically unfounded, and the legislative history offers no explanation.

Finally, a history of closure, by itself, cannot suggest that closure is constitutionally proper. The history of electronic surveillance orders from the 1986 enactment of the ECPA until the present is largely one of secrecy created by legislation, not evidence of a long history of justifiable closure. And, indeed, the prevalence of secrecy actually itself impedes the historical analysis; so few courts have ruled on the record about the propriety of sealing electronic surveillance orders that the historical record is quite thin.[248] Against this background, it is equally likely that closure reflects law enforcement's propensity toward secrecy.[249] Although a "tradition of accessibility implies the favorable judgment of experience,"[250] the inverse is not necessarily true.

## III. THE LOGIC OF PUBLIC ACCOUNTABILITY FOR SURVEILLANCE

The second element of the *Press-Enterprise II* framework requires consideration of "whether public access plays a significant positive role

---

247. United States v. Gonzales, 150 F.3d 1246, 1258 (10th Cir. 1998); *see also* Richmond Newspapers, Inc. v. Commonwealth, 281 S.E.2d 915, 925 (Va. 1981) (finding that a facially-valid statute authorizing closure may be constitutional on its face, but "[u]nless the standard for closure previously discussed has been established in accordance with" adequate procedures, it would be unconstitutional as applied).

248. *See In re* Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 887 (S.D. Tex. 2008) ("No court has yet considered whether electronic surveillance orders fall within the ambit of the First Amendment's right of public access.").

249. *In re* The Search of Fair Fin. v. United States, 692 F.3d 424, 431 ("[W]e do not interpret the fact that the government may in some instances allow documents filed after the execution of the search warrant to become public to be evidence of an historical tradition of accessibility to them.").

250. Richmond Newspapers, Inc. v. United States, 448 U.S. 555, 589 (1980).

in the functioning of the particular process in question."[251] Transparency as a proposed remedy for law enforcement misconduct is not new. Access to documents filed in connection with applications for electronic surveillance plays a positive role by facilitating public understanding of surveillance law and technology, holding law enforcement and prosecutors accountable for uses and abuses of surveillance tools and methods, and making available to the public basic data about the frequency with which police use surveillance authorities.

### *A. Awareness of Surveillance Technology*

Secret surveillance techniques sometimes provide the linchpin of investigations. As police acquire and test out new surveillance techniques, "disclosure 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."[252] This is a legitimate concern, but a narrow one: it may be the case that the police have a compelling interest in maintaining secrecy with regard to *some* surveillance techniques, but it is deeply implausible that every pen register deserves eternal protection from public view.[253] Moreover, recognizing that court orders are public documents does not require police to lay bare their complete arsenal; they may continue to keep from public view sensitive tools and techniques that they may use without judicial approval.[254] Others might see this as an example of just the sort of illegitimate "police exceptionalism" that fails to treat police "as the executive officials they are, subject to the same basic requisites of democracy—namely, transparent, publicly accountable, ex ante regulation."[255]

Transparency is doubly important in the surveillance context because warrantless requests to service providers frequently implicate novel technologies and legal theories. In 2005, the federal government sought an order under the SCA in the Eastern District of New York that would permit the ongoing, prospective disclosure of cell site location

---

251. *Press-Enterprise II*, 478 U.S. 1, 8 (1986).

252. Toomey & Kaufman, *supra* note 22, at 895.

253. *Cf.* Joint Status Report, *supra* note 122.

254. *But see* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016) (discussing how federal procurement circumvents local accountability and oversight mechanisms for police surveillance).

255. Friedman & Ponomarenko, *supra* note 23, at 1833.

information.[256] Magistrate Judge Orenstein demurred, concluding that the government may not lawfully obtain an order authorizing the prospective acquisition of location information unless it demonstrates probable cause.[257] As Judge Orenstein explained, the Communications Assistance for Law Enforcement Act (CALEA) explicitly barred telecommunications carriers from including location information pursuant to pen register and trap and trace authority.[258] Judge Orenstein rejected the government's proposal that it could fuse the statutory authority to conduct prospective surveillance under the Pen/Trap Statute with its authority to collect historical cell site location information under the SCA without impermissibly flouting CALEA.

The same year, across the East River, Magistrate Judge Gorenstein issued an opinion authorizing precisely the relief that Judge Orenstein had declined to grant.[259] Law enforcement's "hybrid theory," which marries the statutory authority to obtain location information under the SCA with the authority to obtain prospective information under the Pen/Trap Statute, created a split among courts.[260]

The so-called "encryption debate" raises additional questions regarding the government's interpretation of its authority to compel assistance under the Pen/Trap Statute. In 2013, the government obtained an order requiring Lavabit, an encrypted email provider, to place a pen/trap device on its system to capture incoming and outgoing traffic on an encrypted email account; Lavabit claimed it could not comply and refused to produce its SSL keys, even after the government obtained a search warrant.[261] Eventually, Lavabit permitted the government to install the pen/trap device it sought, "[b]ut, without the encryption keys, much of the information transmitted to and from Lavabit's servers

256. *In re* Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005), *on reconsideration sub nom. In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005). In the alternative, the government sought the same information under the Pen/Trap Statute.

257. *Id.*

258. *Id.* at 565.

259. *In re* Application of United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 441 (S.D.N.Y. 2005) (finding that a decision that proposed relief was precluded by statute "would constitute a directive that cell site information was not obtainable by any mechanism at all").

260. *See* Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 336 (2011); Timothy Stapleton, *The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More than the Sum of Its Parts?*, 73 BROOK. L. REV. 383, 408 (2007) (discussing split between Orenstein and Gorenstein opinions).

261. *In re* Under Seal, 749 F.3d 276, 281 (4th Cir. 2014).

remained encrypted, indecipherable, and useless."[262] The government explicitly sought to "avoid litigating the issue" of whether Lavabit was required to turn over its keys under the Pen/Trap Statute's provision requiring "technical assistance."[263] To date, that question has not been resolved in a public ruling.

The Lavabit example illustrates the urgent need to understand how the Pen/Trap Statute and the SCA apply to encrypted communications services that—by design—cannot provide detailed information about customers or usage. In two recent drug distribution cases, the government has obtained orders authorizing the installation of a pen/trap device to capture call and messaging details from WhatsApp, a messaging app that uses internet data instead of a wireless network.[264] In one case, the court ordered that, if WhatsApp was not already "equipped with a caller identification option," it must add that feature.[265] In the other case, the court ordered that if WhatsApp "cannot comply," the government could "install and use its own pen register and trap and trace devices" pursuant to the Pen/Trap Statute to obtain information including "date, duration, and timestamp of communication," as well as IP addresses, which can be used to discern location.[266]

In contrast, Apple's iMessage appears to be able to provide "query logs" in response to pen/trap orders that include dates, times, and IP addresses, but it is unable to provide real-time responses or to confirm that a message was actually sent or received.[267] Signal, another encrypted messaging app, appears not to *store* any information about user communications other than "the date and time a user registered with

---

262. *Id.* at 283.

263. *Id.*

264. *See* Application, *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device &/or a Trap & Trace Device &/or Caller Identification Option Device on Tel. No. 1-614-369-5045, United States v. Pen Register, No. 2:16-mj-00254-NMK (S.D. Ohio May 26, 2016), ECF No. 1; Application, *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, United States v. WhatsApp Inc., No. 6:15-cm-60087-EFM-1 (D. Kan. Sept. 16, 2015), ECF No. 1.

265. Order to Service Provider at 2, *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device &/or a Trap & Trace Device &/or Caller Identification Option Device on Tel. No. 1-614-369-5045, United States v. Pen Register, No. 2:16-mj-00254-NMK (S.D. Ohio Sept. 16, 2015), ECF No. 3.

266. Order as to WhatsApp Inc., United States v. WhatsApp Inc., No. 6:15-cm-60087-EFM-1 (D. Kan. May 26, 2016), ECF No. 2.

267. Sam Biddle, *Apple Logs Your iMessage Contacts — And May Share Them with Police*, INTERCEPT (Sept. 28, 2016, 10:00 AM), http://bit.ly/2d9K3nF [https://perma.cc/WPQ4-5LS9].

Signal and the last date of a user's connectivity to the Signal service."[268] It is unclear what Signal could or would produce if it were required to install a pen/trap in order to collect, in real time, additional information about user communications.

These examples illustrate that the government's authority under the Pen/Trap Statute to compel encrypted services to turn over keys or collect additional user information remains unclear. Moreover, as the government seeks to compel encrypted services to comply with court orders in ways that are legally and technologically new, it does so behind closed doors—without even explaining its assertions of authority.

### *B. Understanding Interpretations of Statutory Authority*

In light of the evident difficulties courts experience as they grapple with how to apply old law to new technologies, enhancing access to records reflecting the government's legal reasoning and statutory interpretations would "play[] a particularly significant positive role in the actual functioning of the process" of issuing surveillance orders.[269] Given the proliferation of encrypted messaging services that promise to be more secure than traditional electronic communications, it is particularly striking that the courts have been so silent on the application of surveillance authorities to the acquisition of communications metadata in these new settings. Despite the salience of these questions, there is very little information about how law enforcement actually interprets and uses its authority that is available to Congress, the courts, or the public.

By way of contrast, the public has had access to some rulings on electronic surveillance. For example, the disagreement between Judges Orenstein and Gorenstein regarding the government's ability to acquire prospective location information pursuant to the Pen/Trap Statute is distinctive in part because it was so public. Likewise, several courts have addressed in published opinions whether the Pen/Trap Statute authorizes the government to obtain "post-cut-through dialed digits," the numbers that one might dial after an initial connection is complete, which may include social security numbers, account numbers, numeric voicemail passwords, or extensions.[270] And several magistrate judges have publicly

---

268. *Grand Jury Subpoena for Signal User Data, Eastern District of Virginia*, SIGNAL (Oct. 4, 2016), http://bit.ly/2dYcs2M [https://perma.cc/2NT4-6AJU].

269. *Press Enterprise II*, 478 US 1, 11–12 (1986).

270. *In re* United States, 622 F. Supp. 2d 411, 412 n.2 (S.D. Tex. 2007) (listing cases).

rejected efforts to obtain warrants and court orders authorizing overbroad electronic searches.[271]

However, it remains fairly unusual for magistrate judges to publish decisions regarding government applications for surveillance. Opacity is structurally embedded deep within the courts: magistrate judges, the federal courts' "worker bees," tend not to write as many published opinions as Article III judges.[272] Partly as a result, in many areas in which the government proposes novel constructions of statutory authority to support new investigative methods, "[t]he courts and the Government would all benefit from additional case-law development."[273] As one court recognized, "the best way to test the limit of the Government's authority may be through developed records, trial court opinions on suppression motions, and appellate review."[274]

By informing the public about how the government conducts electronic communications surveillance, release of surveillance records could also foster a better social understanding of technology and enrich the debate about the meaning of Fourth Amendment protections in the information age. As the Fifth Circuit has recognized, "technological changes can alter societal expectations of privacy."[275] But technological change must be publicly known in order for social expectations of privacy to shift accordingly. Indeed, keeping secret information about the scope of the government's surveillance authorities only fuels the argument that users are unaware that they are "voluntarily" or "knowingly convey[ing]" information to third party providers.[276]

Presumptive unsealing of electronic surveillance orders at the conclusion of an investigation would also permit the public to better understand the government's position on its statutory authority. Recognizing a right of access to post-investigation surveillance materials

---

271. *See* Ann E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), http://wapo.st/2l5r9lt [https://perma.cc/J36K-PCRU].

272. *Id.*

273. *In re United States*, 622 F. Supp. 2d at 412–13.

274. *Id.* at 413.

275. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013).

276. *See In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information.").

would also systemically "contribute to ongoing case law"[277] by making the public, legislatures, and courts aware of how surveillance authorities are interpreted and used. As one author points out, "[i]f more magistrates routinely published such decisions, the DOJ's practical monopoly on information about how it uses (or abuses) its surveillance powers would be put to an end, and the *ex parte* expansion of government surveillance authority would be conclusively exposed."[278] Permitting public access to electronic surveillance orders can achieve the same ends without placing additional, onerous burdens on the federal judiciary.

### *C. Improving the Criminal Justice Process*

Increased transparency for electronic surveillance applications and orders is also consonant with an emerging trend of increasing transparency for police departments plagued by misconduct. Sunlight as a remedy for misconduct is visible in settings as disparate as structural reform litigation and the policy debates about deployment of body cameras.[279] Transparent, public filings in support of requests for court orders authorizing surveillance provide a crucial tether between police investigations, which necessarily occur in secret, and the public. In an era in which law enforcement increasingly stands accused of lacking "sufficient democratic authorization,"[280] the closure of court records that authorize police to use intrusive investigative tools is a particularly troubling development.

Public access may improve the criminal process for at least two reasons. First, making police aware that the public will—at some point—be able to read an affidavit offered in support of an application for surveillance may deter police misconduct and perjury. Barry Friedman and Oren Bar-Gill have argued that requiring ex ante search warrants, as a rule, may improve police decision making because police

---

277. Reid Day, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*, 64 U. KAN. L. REV. 491, 520 (2015).

278. Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 590 (2007).

279. *See, e.g.*, Noah Kupferberg, *Transparency: A New Role for Police Consent Decrees*, 42 COLUM. J.L. & SOC. PROBS. 129, 160 (2008) (arguing that the chief value of police consent decrees is in "institutional transparency and the provision of information to the public"); Stephen Rushin, *Structural Reform Litigation in American Police Departments*, 99 MINN. L. REV. 1343, 1396 (2015) (analyzing trends in structural litigation reform); Allyson Scher & Ariel Spierer, *Policing Project to Assist LA: When to Release Body Camera Footage*, POLICING PROJECT (Feb. 1, 2017), http://bit.ly/2lMUroT [https://perma.cc/38S5-ML8B] (describing pressures on police departments to release bodycam footage of police shootings).

280. Barry Friedman & Maria Ponomarenko, *supra* note 23, at 1834.

are aware that their search requests will be scrutinized. Drawing on a significant body of social science research, Friedman and Bar-Gill argue, "the process of seeking a magistrate's approval actually is likely to induce police officers to reach better decisions, either by forcing them to articulate reasons or by leading them to consider what the magistrate will do."[281] Friedman and Bar-Gill believe that police, "cognizant of the fact that their warrant applications will be scrutinized carefully, will not bother filing weak applications."[282] Public access bolsters this rationale: if applications for surveillance were subjected to scrutiny by the public, police may engage in more robust decision making when they seek the relatively low-cost tools available under the SCA and the Pen/Trap Statute.

Electronic surveillance materials are doubly insulated from public view because, unlike traditional Rule 41 warrants, surveillance statutes provide no suppression remedy. While search warrants are "at the center of pre-trial suppression hearings, and suppression issues often determine the outcome of criminal prosecutions,"[283] there is no suppression remedy for violations of the SCA or the Pen Register Statute.[284] Every Circuit to have considered the issue has held that there is a First Amendment right of access to suppression hearings.[285] Indeed, some of the important cases construing the government's authority to obtain certain types of information under the SCA arise from suppression hearings.[286] As a

---

281. Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1642 (2012).

282. *Id.* at 1640.

283. *In re* Search Warrant for Secretarial Area Outside Office of Gunn, 855 F.2d 569, 573 (8th Cir. 1988).

284. United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1548 (2015) ("The Act has a narrow list of remedies, and—unlike the Wiretap Act, *see* 18 U.S.C. § 2515—suppression is not among them."); United States v. Rigmaiden, CR 08-814-PHX-DGC, 2013 WL 1932800, at *10 (D. Ariz. May 8, 2013) (citing United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998)) ("Suppression is not an available remedy for violations of the SCA.").

285. United States v. McVeigh, 119 F.3d 806, 813 (10th Cir. 1997); *In re* Washington Post Co., 807 F.2d 383 (4th Cir. 1986); Application of The Herald Co., 734 F.2d 93, 99 (2d Cir. 1984); United States v. Brooklier, 685 F.2d 1162, 1169–71 (9th Cir. 1982); United States v. Criden, 675 F.2d 550, 557 (3d Cir. 1982); *cf. In re* United States *ex rel.* Pulitzer Pub. Co., 635 F.2d 676, 678 (8th Cir. 1980) (remanding under *Gannett* for failure to make adequate findings justifying closure).

286. *See, e.g.*, United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (holding that "acquisition of historical CSLI from Defendants' cell phone provider did not violate the Fourth Amendment," and suppression was unwarranted); United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("[S]uppression of evidence is not among the remedies available under the Stored Communications Act."); United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) (holding that the government's acquisition of historical cell tower information

result, it should be unambiguous that a First Amendment right of access attaches to electronic surveillance materials filed in connection with suppression hearings. But because exclusion—the traditional ex post remedy for Fourth Amendment violations—is unavailable in the electronic surveillance context, the public right of access to suppression hearings does not really help enhance public understanding of police practices.

The potential for shaming provides another, far more traditional rationale for the functional benefits of transparency. In a recent article, Lara Bazelon discusses a specific type of "judicial shaming" that "occurs when the court takes the prosecutor to task during an oral argument for defending grave misconduct that led to a wrongful conviction."[287] Shaming is a quintessentially "public sanction."[288] Noting that "[t]he second most common cause of wrongful convictions is official misconduct, trailing only false testimony," Bazelon discusses how the Anti-Terrorism and Effective Death Penalty Act stripped federal court judges of their ability to remedy wrongful convictions.[289] In response, she argues, some federal courts are turning to public shaming as a remedy for egregious misconduct by prosecutors. Bazelon quotes Judge Kozinski, who echoed the First Amendment case law when he argued, "[j]udges who see bad behavior before them, especially prosecutors who wield great power and have greater ethical responsibilities, must hold the misconduct up to the light of public scrutiny."[290] Bazelon concludes that the efficacy of public shaming turns on the amount of "public exposure" misconduct receives. "Shaming sanctions require public condemnation. They require spectacle," Bazelon writes.[291]

Holding police individually accountable for misusing investigative tools comports with the history of the Fourth Amendment, as well. During the eighteenth century, targets of unlawful searches brought actions for trespass against the officers who had searched their homes.[292]

---

was not a search, and that suppression was therefore not required); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (same).

287. Lara Bazelon, *For Shame: The Public Humiliation of Prosecutors by Judges to Correct Wrongful Convictions*, 29 GEO. J. LEGAL ETHICS 305, 318 (2016).

288. *Id.*

289. *Id.* at 330.

290. *Id.* at 351.

291. *Id.* at 348.

292. *See, e.g.*, Cuddihy and Hardy, *supra* note 165, at 385 (1980) (describing trespass cases of *Wilkes v. Wood* and *Huckle v. Money*); Davies, *supra* note 163, at 588 ("Because a general warrant was clearly deemed illegal by the framing era, it did not protect either the issuing magistrate or the executing officer against trespass liability.").

By cloaking electronic surveillance in secrecy, courts prevent observers from holding the government or its officers accountable for wrongdoing. But in the area of criminal justice, as the Supreme Court has admonished, public reporting and access to information "guards against the miscarriage of justice by subjecting the police, prosecutors, and judicial processes to extensive public scrutiny and criticism."[293]

### *D. Facilitating Democratic Accountability*

Access to information about electronic surveillance also plays a particularly positive role in the absence of congressional or judicial reporting of aggregate data concerning the use of surveillance authorities. As Paul Schwartz has put it, societal understanding of the scale of electronic surveillance is "largely precluded by the haphazard and incomplete information that the government collects about it."[294]

The paucity of data concerning warrantless electronic surveillance sets it apart from other kinds of law enforcement tools. The Pen/Trap Statute and the SCA lack provisions requiring judicial reporting on the number of times the authority is used each year.[295] Under the Pen/Trap Statute, the Attorney General is required to submit annual reports to Congress on the Department of Justice's use of the authority, but the Department has "routinely failed to submit the required reports."[296] In contrast, the Wiretap Act requires the Administrative Office of U.S. Courts to generate annual reports concerning data on interceptions of oral, wire, or electronic communications under Title III. Likewise, the Foreign Intelligence Surveillance Act requires annual reporting on the number of times the government applies to the Foreign Intelligence Surveillance Court for an order authorizing foreign intelligence surveillance.[297] Nor does the government publicly report, on an annual

---

293. Sheppard v. Maxwell, 384 U.S. 333, 350 (1966).

294. Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 287 (2008).

295. Nevertheless, the data from the FJC study suggests that the numbers are in the thousands, if not the tens of thousands, each year.

296. Naomi Gilens, *New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance*, ACLU (Sept. 27, 2012, 1:32 PM), http://bit.ly/2kQc0pF [https://perma.cc/3EHG-FJD5]. The Stored Communications Act lacks any congressional reporting requirements whatsoever.

297. *See* 18 U.S.C. § 2709 (2012) (requiring semiannual reporting to the Senate and House Judiciary Committees and Select Committees on Intelligence regarding the number of national security letters issued); 50 U.S.C. § 1807 (2012) (requiring the Attorney General to report to the Administrative Office of U.S. Courts and to Congress "(a) the total number of applications made for

basis or otherwise, the number of gag orders it obtains each year to prevent service providers from disclosing the number of requests.[298] In the absence of any kind of comparable data source, public access to electronic surveillance applications and orders, at a minimum, may give the public a sense of the frequency with which the SCA and the Pen/Trap Statute are used.

## IV. COMPELLING NEEDS FOR SECRECY?

If the right of access attaches, the First Amendment requires judicial documents to be unsealed unless the government establishes a "compelling need" for secrecy and shows that sealing is narrowly tailored. How might the right of access be applied to statutes that require or authorize sealing without any factual findings, let alone the demanding showing required under *Press-Enterprise II*?

That the First Amendment standard can only be satisfied by fact-specific showings counsels strongly against statutory standards that create blanket invitations to secrecy. As a general rule, courts must make "specific findings" on the record to demonstrate that the right of access has been overcome.[299] In ongoing investigations, it should be easy for law enforcement to demonstrate that there is a compelling need for secrecy of surveillance materials.[300] When an investigation is ongoing, public access to surveillance documents is likely to play a *negative* role by potentially alerting targets that they are under surveillance.

Nonetheless, the need for secrecy during investigations does not require that the documents filed in connection with those proceedings never see the light of day. To the contrary, courts routinely find that justifications for closure erode over time: even where proceedings are properly closed, the First Amendment may require that a transcript be published "once the danger of prejudice . . . dissipate[s]."[301] When courts grant sealing orders, they may incorporate sunset provisions or requirements that the government inform the court if the "conditions for

---

orders and extensions of orders approving electronic surveillance under this subchapter; and (b) the total number of such orders and extensions either granted, modified, or denied").

298. *See In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013) (nondisclosure order accompanies ninety-seven percent of NSLs).

299. *See* Washington Post v. Robinson, 935 F.2d 282, 288 (D.C. Cir. 1991) (following Second, Fourth and Ninth Circuits in requiring courts to make "specific findings . . . on the record" to justify sealing plea agreements).

300. *In re* U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 292 (4th Cir. 2013).

301. Gannett Co. v. DePasquale, 443 U.S. 368, 393 (1979).

unsealing" occur.[302] Even grand-jury materials, which are inarguably subject to exceptionally strong secrecy requirements, might someday become public.[303]

The effect of blanket secrecy requirements like those in the Pen/Trap Statute is to categorically and indefinitely shield records long after any interest in secrecy, no matter how compelling, has dissipated. These secrecy requirements ignore that facts change. Where a criminal investigation has come to an end—whether it results in an indictment or no judicial action at all—there is no obvious government interest in secrecy sufficiently compelling to justify sealing tens of thousands of judicial documents. Once an investigation is concluded, the right of access can shine a light on law enforcement activity that may otherwise remain secret indefinitely. Applying the constitutional test to electronic surveillance orders strongly suggests that the First Amendment right of access should attach to electronic surveillance applications and orders after an investigation has terminated.

Now, several cases are challenging the long-term, unjustified sealing of pen registers and other electronic surveillance applications and orders. In recent litigation in the District of Columbia, a journalist sought access to each application, affidavit, and court order under the Pen/Trap Statute and the SCA.[304] In response, the government published a list of the docket information for pen registers and trap-and-trace orders issued in 2012—a total of 235 matters—and proposed that only 10% of the matters ought to be unsealed in whole or in part.[305] While the court ultimately concluded that a First Amendment right of access did not attach to the records sought, it did recognize that the public had a common law right that required the clerk's office and the prosecutor's office to publish additional information concerning surveillance applications and orders.[306] Ongoing litigation in the Northern District of

---

302. United States v. Dwyer, 629 F. App'x 85 (2d Cir. 2015); *see also* T. S. Ellis, III, *Sealing, Judicial Transparency and Judicial Independence*, 53 VILL. L. REV. 939, 949 (2008) ("[E]very order sealing records should explicitly limit its own duration or, alternatively, require the party seeking protection to reappear and reestablish the necessity of the seal.").

303. Carlson v. United States, 837 F.3d 753, 767 (7th Cir. 2016) (holding that district courts retain discretion to disclose historical grand jury materials).

304. Petition, *In re* The Application of Jason Leopold to Unseal Certain Electronic Surveillance Applications and Orders, No. 1:13-mc-00712-BAH (D.D.C. July 16, 2013), ECF No. 1.

305. Fourth Joint Status Report, *In re The Application of Jason Leopold* (D.D.C. Jan. 17, 2017), ECF No. 28.

306. *In re* Leopold to Unseal Certain Elec. Surveillance Applications & Orders, No. 13-MC-00712, 2018 WL 1129660, at *32 (D.D.C. Feb. 26, 2018) (recognizing a prospective right of access under the common law).

California is also seeking docketing and unsealing of court records related to matters arising under the Wiretap Act, the SCA, and the Pen/Trap Statute.[307]

A second proposed justification for secrecy stems from concerns about the individual privacy of those who are targeted. Communications surveillance records might be particularly sensitive and revelatory, and access to documents pertaining to surveillance may invade individual privacy. Many have noted that even "transactional" records related to communication can disclose highly sensitive information related to political, religious and expressive associations,[308] eroding the contested boundary between "content" and "metadata."[309] Because surveillance orders do not require probable cause, many targets of surveillance may not even be criminal suspects.

Others have noted that public access to pretrial judicial documents may be particularly invasive in cases in which charges against an individual are dropped, or the defendant is ultimately acquitted:

> [E]ven in cases where charges were wrongfully brought—a case of mistaken identity, perhaps, or simply a misunderstanding—the record of that individual's history in the criminal justice system will remain. Rarely will this record note that the charges were dismissed, or that the individual was found to be innocent.[310]

One recent disclosure is instructive. In May 2012, the Associated Press and other news organizations published an article concerning a

---

307. *See* discussion *supra* at notes 17–19. In an earlier case seeking access to historical applications and orders under the Pen/Trap Statute, a federal court ruled in a minute order that the documents at issue "are not subject to the First Amendment Right of Access," apparently on the basis that an investigation was ongoing. United States v. Pen Register, No. 2:10-mj-01235 (S.D. Tex. June 4, 2015). In the one case in which the United States did not oppose the unsealing, the Court determined that the Wall Street Journal's motion to gain access was moot. Sealed Matter, No. 2:07-mc-127 (S.D. Tex. Aug. 25, 2015); *see also* Brian L. Owsley, *To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 CAL. L. REV. CIRCUIT 259 (2014).

308. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 744 (2008) ("Current legal doctrine, which centers on 'privacy' and hence on protecting the content of communications, does not adequately account for the extent to which relational surveillance threatens to chill expressive association in today's networked world.").

309. *See, e.g.*, Freiwald, *supra* note 210, at 70 (arguing that the binary content-metadata distinction has "dire consequences for privacy on the Internet"); Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1453 (calling for the "abandonment" of the "envelope analogy" that calls for leaving metadata unprotected).

310. Amanda Conley et al., *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772, 783–84 (2012).

disrupted terrorist plot to use an upgraded "underwear bomb" on an aircraft.[311] After the Associated Press published its story, the government confirmed the account.[312] The FBI then opened a leak investigation of the disclosure, which implicated sensitive and classified national security information.[313] In the course of investigating, the FBI secretly subpoenaed two months of telephone records from the Associated Press.[314] After receiving the records, the FBI then applied for an SCA order compelling Google to turn over email records belonging to one of the reporters.[315]

The subpoenas became public less than a week later, and the leaker in that case—Donald Sachtleben—pleaded guilty in September 2013.[316] But the application for the reporter's email records remained under seal until September 2017, when the Reporters Committee for Freedom of the Press successfully moved to unseal it. Although the reporter's name and the name of the publication are redacted, there are more than enough details in the records to reconstruct the identities of both. Indeed, if this episode were not already public, this form of disclosure could raise substantial privacy concerns. But the fact that the records remained sealed even after the investigation was made public and had been closed for four years simply illustrates the overbreadth of the secrecy requirement.

Publicizing surveillance-related court records, therefore, is not without its drawbacks as a policy matter. But the fact that surveillance

---

311. Adam Goldman & Matt Apuzzo, *US: CIA Thwarts New Al-Qaida Underwear Bomb Plot*, YAHOO! (May 7, 2012), https://www.yahoo.com/news/us-cia-thwarts-al-qaida-underwear-bomb-plot-200836835.html [https://perma.cc/5B85-D33N]; Greg Miller & Karen DeYoung, *Al-Qaeda Airline Bomb Plot Disrupted, U.S. Says*, WASH. POST (May 7, 2012), https://www.washingtonpost.com/world/national-security/cia-disrupts-airline-bomb-plot/2012/05/07/gIQA9qE08T_story.html [https://perma.cc/P2F2-T2SE]; Eyder Peralta, *CIA Thwarts New, More Sophisticated Underwear Bomber*, NPR (May 7, 2012), www.npr.org/sections/thetwo-way/2012/05/07/152207969/reports-cia-thwarts-new-more-sophisticated-underwear-bomber.

312. Associated Press, *CIA 'Foiled Al-Qaida Bomb Plot' Around Anniversary of Bin Laden Death*, GUARDIAN (May 7, 2012), https://www.theguardian.com/world/2012/may/07/cia-al-qaida-bomb-plot [https://perma.cc/76BB-N5YG] ("The White House confirmed the story after the AP published it on Monday afternoon.").

313. Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, N.Y. TIMES (Sept. 23, 2013), www.nytimes.com/2013/09/24/us/fbi-ex-agent-pleads-guilty-in-leak-to-ap.html.

314. Sari Horwitz, *Under Sweeping Subpoenas, Justice Department Obtained AP Phone Records in Leak Investigation*, WASH. POST (May 13, 2013), http://wapo.st/10uGlF6 [https://perma.cc/SC66-QAD4].

315. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:13-mc-00460-AK*SEALED* (D.D.C. May 7, 2013), ECF No. 1.

316. Savage, *supra* note 313.

materials in individual cases may implicate individual privacy rights does not mean that there is no history or logic of access to those materials. As the Fourth Amendment history illustrates, the public has long had access to information about the execution of searches—information that was critical to understanding how and when government searches were abusive and unconstitutional. Implicit in this history is the idea that the Fourth Amendment's protections are endangered when searches are executed in secret. As the Second Circuit noted when articulating the need for safeguards for "sneak and peek" searches, secret searches increase the risk that "officers will exceed the bounds of propriety without detection."[317]

In specific cases, individual privacy interests might well involve a compelling need for secrecy that could outweigh the public's right of access to surveillance materials. Courts can address this by applying the constitutional standard for closure of court records. Nor is this an all-or-none project: courts can also use traditional, narrowly tailored methods of safeguarding privacy in public records, such as the use of redactions to anonymize the identifying details of innocent surveillance targets. Critically, however, the First Amendment demands that judges make these determinations on the facts of specific cases, not on the basis of general principles.

More to the point, this argument raises a graver issue that lies at the very core of the need for increased transparency and public oversight of surveillance. It is a matter of the utmost public concern if law enforcement is routinely targeting innocent individuals for secret surveillance without notice. The government invades those individuals' privacy when they are targeted for surveillance, not only when it is later exposed. Efforts to shield that surveillance from view tend to preserve what Patrick Toomey and Brett Max Kaufman called the "notice paradox": "the people the government deprives of notice will never *know* that it chose not to provide notice to them."[318] The position is akin to New York City's defense of its programmatic surveillance of Muslims after September 11: the plaintiffs who were under surveillance were injured, not by the surveillance itself, but by the Associated Press's reporting of the program. This absurdist stance, as the Third Circuit aptly described it, amounts to: "[w]hat you don't know can't hurt you. And, if you *do* know, don't shoot us. Shoot the messenger."[319] Put

317. United States v. Villegas, 899 F.2d 1324, 1336 (2d Cir. 1990).

318. Toomey & Kaufman, *supra* note 22, at 848.

319. Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015).

another way, the government should not be able to secretly surveil innocent people and then avoid scrutiny by asserting that revealing the government's privacy-invasive activity would infringe on their privacy.

## CONCLUSION

Widespread sealing and secret docketing practices for materials related to the SCA and pen register/trap and trace orders obscure key data about law enforcement's use of surveillance, including legal interpretations. Recognizing that a First Amendment right of access attaches to these materials would not, however, open all of them to immediate scrutiny. A right of access that attaches after an investigation has concluded would not jeopardize law enforcement techniques or the integrity of the ex parte proceedings seeking surveillance. Far from it—some additional sunshine in this dimly lit area would not only have a salutary effect on surveillance and policing, but it is also consonant with historical practice, as the First Amendment requires. And in truly compelling circumstances, the First Amendment right of access might yield to law enforcement's compelling interest in secrecy, even after an investigation has ended, to keep the materials under seal.

In other words, courts should treat surveillance orders like other court records under the First Amendment. Applying these generally held principles of constitutional law to surveillance orders would rectify the unexplained disparity that exists between access to surveillance orders and access to other documents filed in connection with pretrial criminal proceedings.