Michigan Law Review

Volume 123 | Issue 8

2025

Law Enforcement Privilege

Rebecca Wexler
Columbia Law School

https://doi.org/10.36644/mlr.123.8.law

LAW ENFORCEMENT PRIVILEGE

Rebecca Wexler

TABLE OF CONTENTS

LAW ENFORCEMENT PRIVILEGE

*Rebecca Wexler**

You can't question a secret you haven't been told. The criminal legal system depends on fair and open proceedings to expose and regulate unlawful and unconstitutional police conduct through the courts. If police can use claims of secrecy to systematically thwart criminal defendants' access to evidence, judicial review will fail. And yet that is exactly what is happening under a common-law doctrine called the "law enforcement privilege." The privilege empowers police and prosecutors to rely on the results of secret investigative methods while withholding information from the defense about how those methods work. It risks perpetuating unconstitutional conduct, enabling wrongful convictions, and rendering Fourth Amendment, Sixth Amendment, Brady*, and statutory discovery laws moot. At the same time, it has a non-frivolous policy rationale. If all police investigative methods were public information, then more people committing crimes could evade detection.*

How can a better balance be struck? This Article argues that current law enforcement privilege doctrine creates a dangerously boundless police secrecy power because of a subtle conceptual collapse: The policy rationale itself is mistakenly used as the test for assessing claims of privilege. The Article recommends that courts instead evaluate privilege claims by reference to the marginal risk of leaking posed by in-court disclosure. Specifically, judges should demand to know what conditions law enforcement previously imposed on access to the information. The answer to that question can be adjudicated publicly without jeopardizing a legitimate privilege claim and will help judges detect mistaken, exaggerated, pretextual, or fraudulent claims to the privilege. Further, even when law enforcement has taken care with the information, if a court-ordered protective order can match or exceed the safeguards that law enforcement itself previously maintained, then judges should default to ordering disclosure. The Article concludes by suggesting a theory of the role of confidentiality in privilege law.

---

* Professor of Law, Columbia Law School. Thank you to Elena Chachko, Edward Cheng, Colleen Chien, Bryan Choi, Catherine Crump, Judge Jeremy Fogel, Mark Gergen, Aziz Huq, Edward Imwinkelried, Orin Kerr, Christina Koningisor, Ronald Lee, Anna Lvovsky, Erin Murphy, Ngozi Okidegbe, Neil Richards, Daniel Richman, Andrea Roth, Pam Samuelson, Paul Schwartz, Elisabeth Semel, Jonathan Shaub, Jonathan Simon, Maneka Sinha, Judge Stephen Smith, Molly Van Houweling, Rory Van Loo, Charles Weisselberg, and Ben Wizner for helpful comments on prior drafts. This Article benefited greatly from presentations at Berkeley, Columbia, Denver, Fordham, Irvine, Pennsylvania, Vanderbilt, and Yale Law Schools, as well as the Privacy Law Scholar's Conference and the Decarceration Scholar's Workshop. Thank you to my wonderful team of research assistants, Alexa Daugherty, Izzy Simon, Cheyenne Smith, Tyler Takemoto, and Daniela Wertheimer; to Gilad Edelman for invaluable editorial guidance; and to the editors of the *Michigan Law Review* for their careful and insightful editorial input.

INTRODUCTION

In *Mapp v. Ohio*, police used a fake warrant to search a home.[1] In *Katz v. United States*, police wiretapped a phone booth without getting a warrant.[2] In *Riley v. California*, police warrantlessly searched a cell phone.[3] And in *Carpenter v. United States*, police collected 12,898 data points from one person's cell phone location information, again without a warrant.[4] In each case, a criminal defendant challenged the police conduct in an adversarial hearing, and the Supreme Court ruled that the conduct violated the Fourth Amendment.

These landmark rulings, and many more like them, have defined the modern Fourth Amendment. None of them would exist if the police conduct at issue had been secret. If police had concealed their warrant fraud, trespassory wiretapping, cell phone searches, and bulk location tracking from these defendants, these tactics could have continued indefinitely. The criminal legal system depends on fair and open proceedings to expose and regulate unlawful and unconstitutional police conduct through the courts. If police can use claims of secrecy to systematically thwart defense access to evidence, judicial review will fail.

And yet, that is exactly what is happening under an obscure but powerful common-law doctrine called the "law enforcement privilege." This evidentiary privilege empowers police and prosecutors to rely on the results of secret investigative methods while concealing how those methods work from the defendants against whom they are used. The privilege is designed to apply to methods that would become ineffective if generally known. It is a qualified privilege, meaning that courts first decide whether the privilege applies and then balance the competing interests in secrecy and disclosure in any given case.[5] Though not always invoked and not always upheld, the privilege has been cited in over eleven hundred federal opinions in the past forty years and has almost certainly successfully concealed police conduct in many more discovery disputes that did not culminate in written opinions.[6]

This Article argues that present doctrine creates a dangerously boundless police secrecy power. Practically speaking, what currently limits threshold claims to the privilege is not law but rather the technical feasibility of keeping an investigative method secret while deploying it in the field. The Article recommends that courts instead constrain law enforcement's secrecy power by tying privilege claims to the safeguards that law enforcement itself imposed on

1. Mapp v. Ohio, 367 U.S. 643, 645 (1961).
2. Katz v. United States, 389 U.S. 347, 348–49, 356 (1967).
3. Riley v. California, 573 U.S. 373, 378–79 (2014).
4. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
5. Tuite v. Henry, 181 F.R.D. 175, 176–77 (D.D.C. 1998).
6. *See infra* notes 80–87 and accompanying text.

the information before the dispute arose. This approach offers an array of substantive and procedural benefits[7] and finds helpful precedents in other privilege doctrines, trade secret law, and secrecy scholarship.[8]

Our nation is struggling to grapple with secrecy that enables law enforcement misconduct. Bodycam and cell phone footage have exposed horrific police murders and violence, the planting of fake evidence, and other gross abuses that might otherwise have been suppressed.[9] The White House blacklisted the spyware company NSO Group after it sold secret hacking software to foreign governments that used it surreptitiously to surveil human rights activists, journalists, and dissidents.[10] Protests following George Floyd's murder by police led to, among other achievements, increased public access to police misconduct records.[11] And President Biden's "Executive Order on Advancing Effective, Accountable Policing" set forth transparency through "public reporting" as a primary policy to achieve equitable, accountable, constitutional, and effective policing.[12]

This work is urgent but incomplete. Scholars and practitioners addressing the clash between police secrecy and transparency interests have focused pri-

---

7. *See infra* notes 297–319 and accompanying text.

8. *See infra* notes 320–333 and accompanying text.

9. *See, e.g.*, Bernd Debusmann, Jr., *Tyre Nichols Video: What the Footage of Police Beating Shows*, BBC (Sept. 9, 2024) https://www.bbc.com/news/world-us-canada-64422576 [perma.cc/VN7W-7V2B]; Evan Hill, Ainara Tiefenthäler, Christiaan Triebert, Drew Jordan, Haley Willis & Robin Stein, *How George Floyd was Killed in Police Custody*, N.Y. TIMES (Jan. 24, 2022) https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html [perma.cc/LM2H-LASC]; *Black Lives Upended by Policing: The Raw Videos Sparking Outrage*, N.Y. TIMES (Apr. 19, 2018) https://www.nytimes.com/interactive/2017/08/19/us/police-videos-race.html [perma.cc/YX93-44KE] (collecting videos of the police killings of Danny Ray Thomas, Stephon Clark, Carnell Snell Jr., Keith Lamont Scott, Terence Crutcher, Paul O'Neal, Joseph Mann, Philando Castile, Alton Sterling, Christian Taylor, Samuel Dubose, Sandra Bland, Freddie Gray, Walter L. Scott, Tamir Rice, Laquan McDonald, Michael Brown, Eric Garner, Antonio Zambrano-Montes, Ricardo Diaz-Zeferino, and videos of police violence against Johnnie Jermaine Rush, Richard Hubbard III, Demetrius Bryan Hollins, Nania Cain, Dejuan Hall, Jacqueline Craig, Charles Kinsey, James Blake, and multiple Black children); Jay Stanley, *Baltimore Police Caught by Their Own Body Cameras Planting Evidence: Lessons*, ACLU (Aug. 7, 2017) https://www.aclu.org/news/privacy-technology/baltimore-police-caught-their-own-body-cameras [perma.cc/W89L-PVBQ].

10. David E. Sanger, Nicole Perlroth, Ana Swanson & Ronen Bergman, *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. TIMES (Nov. 3, 2021) https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html [perma.cc/PN44-AZJD]; *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, U.S. DEP'T OF COM. (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [perma.cc/4QX2-AZSY].

11. *See, e.g.*, Ashley Southall, *N.Y.P.D. Releases Secret Misconduct Records After Repeal of Shield Law*, N.Y. TIMES (Oct. 13, 2021), https://www.nytimes.com/2021/03/08/nyregion/nypd-discipline-records.html [perma.cc/9EYR-P7JQ].

12. Exec. Order No. 14,074, 3 C.F.R. § 371 (2023).

marily on public records laws, leaving evidentiary privileges largely unexamined.[13] This oversight is especially concerning given the high stakes of privilege law for both police accountability and the accurate resolution of criminal cases.

Secret investigative methods may be substantially more invasive and less reliable than police and prosecutors claim or even realize.[14] By impeding judicial review of these methods,[15] the law enforcement privilege risks perpetuating unconstitutional conduct, enabling wrongful convictions, and rendering Fourth Amendment,[16] Sixth Amendment, *Brady*,[17] and statutory discovery laws moot. Moreover, law enforcement officials can abuse the secrecy power if they overclaim the privilege or lie about their investigative methods,[18] whether to conceal mistakes and wrongdoing or simply to shield methods on which they rely from adversarial scrutiny and judicial review.[19]

One classic story of abuse concerns a cell phone surveillance technology known as a "Stingray." A Stingray, also called a cell site simulator, tricks physically proximate phones into divulging information.[20] For over a decade,[21] law

13. *Compare* Christina Koningisor, *Police Secrecy Exceptionalism*, 123 COLUM. L. REV. 615 (2023), *and* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. 917 (2021), *and* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016), *with* Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503 (2019).

14. On broad societal and democratic harms of secret surveillance programs that are difficult for courts to review, see Amna Akbar, *Policing "Radicalization"*, 3 U.C. IRVINE L. REV. 809, 851–54 (2013), and Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951 (2013).

15. Certainly, criminal courts are not, and should not be, the sole institutional solution for vetting law enforcement investigative methods. Legislative, regulatory, and civilian oversight entities also play important roles. *See, e.g.*, N.Y. Exec. L. § 995-A (McKinney 2022) (establishing forensic oversight commission); Sharon R. Fairley, *Survey Says: The Development of Civilian Oversight of Law Enforcement Skyrockets in the Wake of George Floyd's Killing*, 31 S. CAL. REV. L. & SOC. JUST. 283 (2022) (documenting rise in civilian oversight of municipal police); May M. Cheh, *Legislative Oversight of Police: Lessons Learned from an Investigation of Police Handling of Demonstrations in Washington, D.C.*, 32 J. LEGIS. 1 (2005).

16. *See* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016).

17. Brady v. Maryland, 373 U.S. 83 (1963).

18. *Cf.* Hampton v. Hanrahan, 600 F.2d 600, 639–42 (7th Cir. 1979).

19. Alex Kingsbury, *Daniel Ellsberg Never Ran Out of Secrets*, N.Y. TIMES (Mar. 24, 2023), https://www.nytimes.com/2023/03/24/opinion/international-world/ellsberg-nuclear-war-ukraine.html%20 [perma.cc/V7ZU-JHQG].

20. Mariana Oliver & Matthew B. Kugler, *Surveying Surveillance: A National Study of Police Department Surveillance Technologies*, 54 ARIZ. ST. L.J. 103, 130–34 (2022).

21. State FOIA Aff. of Bradley S. Morrison at 2 (Apr. 11, 2014), https://www.documentcloud.org/documents/1208337-state-foia-affidavit-signed-04112014.html [perma.cc/NSJ2-YBWE].

enforcement officers across the country kept Stingray devices secret while relying in court on evidence generated through their use.[22] Police officers routinely used these surveillance devices without a warrant,[23] made misleading omissions in warrant affidavits and pen register applications,[24] lied about the technology in probable cause hearings,[25] and refused to answer questions about the technology in courtroom testimony.[26] In some instances, when courts denied the privilege claims, prosecutors dropped criminal cases instead of complying with orders to disclose information about the devices.[27] Contracts for the sale of these devices required police purchasers to withhold information about how the technology works, including "in response to court ordered disclosure."[28] Contractual promises to disobey court-ordered disclosures are—or at least should be—unenforceable as a matter of contract law.[29] But privilege law does provide a defense against court-ordered disclosures. The power that gave the Stingray's contractual gag provision legal weight, even in the face of a contrary court order, was the law enforcement privilege.[30]

When the secrecy was finally exposed (extraordinarily, by a *pro se* criminal defendant who spent years in prison researching the police department that

22. Cyrus Farivar, *FBI Would Rather Prosecutors Drop Cases than Disclose Stingray Details*, ARS TECHNICA (Apr. 7, 2015, 4:35 PM), https://arstechnica.com/tech-policy/2015/04/fbi-would-rather-prosecutors-drop-cases-than-disclose-stingray-details [perma.cc/LZT7-XPE3].

23. *Id.*

24. Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is a Stupid Thing to Do"*, ARS TECHNICA (June 20, 2014, 11:38 AM), https://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do [perma.cc/E6MH-RT5E].

25. Mike Masnick, *New Emails Show that Feds Instructed Police to Lie About Using Stingray Mobile Phone Snooping*, TECHDIRT (June 20, 2014, 12:03 PM), https://www.techdirt.com/2014/06/20/new-emails-show-that-feds-instructed-police-to-lie-about-using-stingray-mobile-phone-snooping [perma.cc/2RV4-V9CF].

26. Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, BALT. SUN (June 1, 2019, 5:11 PM), https://www.baltimoresun.com/2014/11/17/judge-threatens-detective-with-contempt-for-declining-to-reveal-cellphone-tracking-methods [perma.cc/953A-X4LD].

27. Sam Adler-Bell, *What's Behind the FBI's Obsessive "Stingray" Secrecy?*, CENTURY FOUND. (Apr. 9, 2015), https://tcf.org/content/commentary/whats-behind-the-fbis-obsessive-stingray-secrecy [perma.cc/4ED7-63HU]; Email from Christopher M. Allen, FBI Office for Pub. Affs., to Cyrus Farivar, Senior Tech Pol'y Rep., Ars Technica (May 15, 2015, 5:59 AM), https://www.documentcloud.org/documents/2082240-urgent-copy-of-stingray-statement.html [perma.cc/ES7J-UZC7].

28. Letter from Christopher M. Piehota, Special Agent in Charge, FBI, to Scott R. Patronik, Chief, Eric Cnty. Sheriff's Office, Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations at 3 (June 29, 2012), https://www.documentcloud.org/documents/1727748-non-disclosure-agreement.html#document/p3/a212394 [perma.cc/LGU5-D5FV].

29. Fenton, *supra* note 26.

30. *See* United States v. Rigmaiden, 844 F. Supp. 2d 982, 996–1005 (D. Ariz. 2012); State FOIA Aff. of Bradley S. Morrison, *supra* note 21, at 1.

arrested him),[31] it drew widespread criticism from across the political spectrum[32] and fueled nationwide litigation campaigns.[33] Legal scholars lambasted this "unacceptable secrecy"[34] as an illustration that "far too much of policing lives in a dark hole of ignorance."[35] Multiple courts held that the Fourth Amendment requires police to obtain a warrant before using a Stingray.[36] These decisions, combined with public opinion, forced the Departments of Justice and Homeland Security to adopt policies requiring warrants before deploying the surveillance devices.[37] Bipartisan congressmembers introduced

---

31. Extraordinarily, this defendant spent years in prison researching the police department that arrested him. Rebecca Wexler, *Code of Silence: How Private Companies Hide Flaws in the Software That Governments Use to Decide Who Goes to Prison and Who Gets Out*, WASH. MONTHLY (June 11, 2017), https://washingtonmonthly.com/2017/06/11/code-of-silence [perma.cc/AS82-B576].

32. The ACLU tracked police purchase of Stingrays in the past, and the Electronic Frontier Foundation does so currently. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://web.archive.org/web/20241001002008/https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [https://perma.cc/5U4W-YKBK] (last updated Nov. 2018); *Atlas of Surveillance*, ELEC. FRONTIER FOUND., https://atlasofsurveillance.org/atlas [perma.cc/LX3E-LGQS]. Conservative commentators have asserted that the "level of non-disclosure regarding StingRay devices is unusually high." Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything*, FEDERALIST SOC'Y REV., Feb. 2016, at 29, 32, https://fedsoc.org/fedsoc-review/stingray-technology-and-reasonable-expectations-of-privacy-in-the-internet-of-everything [perma.cc/2BCZ-E8XZ]. For criticisms in the national press, see Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST (Mar. 27, 2013, 8:58 PM), https://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html [perma.cc/7ZMY-W8C6].

33. *E.g.*, Alexia Ramirez, *ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices*, ACLU (May 27, 2020), https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices [perma.cc/ZM93-2PAD].

34. Barry Friedman, *Secret Policing*, 2016 U. CHI. LEGAL F. 99, 100–05.

35. Barry Friedman & Elizabeth G. Jánszky, *Policing's Information Problem*, 99 TEX. L. REV. 1, 33, 49–50 (2020); *accord* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 28–29 (2017); Friedman, *supra* note 34, at 100–05; 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, 35–39 (2014).

36. *E.g.*, United States v. Ellis, 270 F. Supp. 3d 1134, 1142–46 (N.D. Cal. 2017); United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016); Jones v. United States, 168 A.3d 703, 707 (D.C. Ct. App. 2017); People v. Gordon, 68 N.Y.S.3d 306, 310–11 (Sup. Ct. 2017).

37. *See* U.S. DEPT. OF HOMELAND SEC., POL'Y DIRECTIVE 047-02, DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY 4 (2015); Press Release, Off. of Pub. Affs. U.S. Dep't of Just., Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [perma.cc/4SVL-URCV].

the Cell-Site Simulator Warrant Act.[38] Most recently, a report by the Department of Homeland Security Office of Inspector General revealed that, despite these reform efforts, the Secret Service and Immigration and Customs Enforcement still did not always comply with the statutes and policies regulating Stingray use.[39] The upshot is that for more than a decade, the law enforcement privilege enabled police to conduct what multiple courts have since deemed unconstitutional, warrantless searches, without facing either political oversight or meaningful judicial scrutiny. It is impossible to know how frequently the privilege conceals other misconduct that has yet to be revealed.

Constitutionality is one thing; accuracy is another. The law enforcement privilege risks entrenching investigative methods and forms of evidence that are flawed or inaccurate by preventing defendants from putting them to the test. The privilege (like privileges generally) applies to every stage of a case, from pretrial suppression motions to post-conviction proceedings.[40] Hence, the privilege can block adversarial scrutiny of investigative methods even when the results of those methods are introduced as part of the government's case-in-chief at trial. It is worth emphasizing this point: The privilege is not just an issue at suppression hearings; it also reaches substantive evidence of guilt or innocence. When the results of a method are ultimately introduced at trial, the method veers from investigative to forensic.[41] In such circumstances, the law enforcement privilege still applies. Hence, the law enforcement privilege also risks propagating flawed or fraudulent forensic methods and unreliable evidence at trial.

For instance, multiple courts have upheld the law enforcement privilege to prevent criminal defense experts from testing internet monitoring software programs, even when outputs from those programs are used as direct evidence of guilt.[42] In *United States v. Pirosko*[43]—a Sixth Circuit opinion that has been cited over four hundred times[44] and characterized by one federal court as

38. Caroline Haskins, *There Are No Laws Restricting "Stingray" Use. This New Bill Would Help.*, BUZZFEED NEWS (June 17, 2021, 10:30 AM), https://www.buzzfeednews.com/article/carolinehaskins1/new-law-restrict-stingray-surveillance-use [perma.cc/3GLZ-SCL9].

39. OFF. OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., OIG-23-17, SECRET SERVICE AND ICE DID NOT ALWAYS ADHERE TO STATUTE AND POLICIES GOVERNING USE OF CELL-SITE SIMULATORS (REDACTED) 6 (2023).

40. *See* FED. R. EVID. 1101(c).

41. *See* Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 841–42 (2022) (noting gray area between investigative and forensic technologies).

42. *E.g.*, Motion to Compel Discovery at 9, United States v. Clements, No. 15-cr-275 (N.D. Ohio Jan. 18, 2016), ECF No. 17; United States v. Clements, No. 15-CR-275 (N.D. Ohio Jan. 27, 2016), ECF No. 19 (order denying motion to compel discovery); United States v. Pirosko, 787 F.3d 358, 366–67 (6th Cir. 2015); United States v. Pirosko, No. 12-cr-00327, at 7 (N.D. Ohio, Aug. 13. 2023), ECF No. 33 (order denying Defendant's Motion to Compel Discovery and Request to Extend Pretrial Motion Deadline)

43. *Pirosko*, 787 F.3d 358.

44. *Citing References to* United States v. Pirosko, WESTLAW, https://1.next.westlaw.com/Document/Ifb4dfc06ffdb11e4a807ad48145ed9f1/View/FullText.html (last visited June 26, 2021) (follow "Citing References" hyperlink).

spawning a "line of cases" that deny criminal defense teams "access to confidential government investigative software"[45]—the defense sought to test a program's "reliability and capabilities,"[46] both to support a suppression motion and to contest the accuracy of the government's evidence of guilt.[47] The district and appellate courts both relied on the privilege to deny the defendant's request.[48] There are many other cases with similar results.[49] These cases prompted Human Rights Watch to send a letter to the Department of Justice expressing concern over surveillance software programs that might be providing "secret law enforcement access to personal data," and that have unknown error rates.[50]

The prospect of law enforcement concealing flaws or fraud in evidence of guilt is no idle concern. According to the National Registry of Exonerations, over a quarter of the wrongful convictions recorded in its database involved

---

45. United States v. Gonzales, No. CR-17-01311-001-PHX, 2019 WL 669813, at *3 (D. Ariz. Feb. 19, 2019).

46. Brief of Appellant Joseph J. Pirosko at 18–19, *Pirosko*, 787 F.3d 358 (No. 14-3402).

47. *Pirosko*, 787 F.3d at 365; United States v. Pirosko, No. 12-cr-00327, at 2 (N.D. Ohio Aug. 13, 2013), ECF No. 33.

48. *Pirosko*, 787 F.3d at 364, 366–67.

49. For instance, in *United States v. Clements*, a federal district court denied a criminal defendant access to an executable copy of a surveillance software program for testing after the government opposed the defendant's discovery motion by asserting the law enforcement privilege. The district court reached this finding even though outputs from the software formed the sole evidence of guilt for multiple criminal charges in the case. United States v. Clements, No. 15-cr-00275 (N.D. Ohio Jan. 27, 2017), ECF No. 19 (order denying motion to compel); Motion to Compel Discovery at 9, United States v. Clements, No. 15-cr-00275 (N.D. Ohio Jan. 18, 2016), ECF No. 17; Government's Memorandum in Opposition to Defendant's Motion to Compel Discovery at 3–6, United States v. Clements, No. 15-cr-00275 (N.D. Ohio Jan. 26, 2016), ECF No. 18. And in *United States v. Chiaradio*, a federal district court relied in part on the privilege to deny a criminal defendant access to the source code for a surveillance software program, despite admitting outputs from that software into evidence as part of the government's case-in-chief at trial. *See* United States' Objection & Response to Defendant's Motion to Compel at 13, United States v. Chiaradio, No. 09-cr-069 (D.R.I. Jan. 6, 2010), ECF No. 43 (arguing that even if the defense established the materiality of the software, "the defendant has no right to have access to propriety [sic] investigative techniques . . . [and] is not entitled to review or access material covered by the law enforcement privilege"); United States' Notice of Intent to Use Evidence and Request for an Evidentiary Hearing on the Defendant's Motion to Compel at 3, United States v. Chiaradio, No. 09-069 (D.R.I. Mar. 31, 2010), ECF No. 50 (asserting that prosecution "wished to use EP2P evidence during its case-in-chief" because "[s]uch evidence is essential to proving the elements of the government's case"); Supplemental Memorandum of Law in Support of Motion to Compel at 40–41, United States v. Chiaradio, No. 09-069 (D.R.I. June 3, 2010), ECF No. 55 (contesting law enforcement privilege); Docket Minute Entry at *11, United States v. Chiaradio, No. 09-069 (D.R.I. July 21, 2010) (denying defendant's motion to compel source code following the government's invocation of the law enforcement privilege); Docket Minute Entry at *13, United States v. Chiaradio, No. 09-069 (D.R.I. Nov. 1, 2010) (granting government's motion in limine and admitting government expert testimony about the results of EP2P surveillance software).

50. Letter from Hum. Rts. Watch to U.S. Dep't of Just. 2 (Feb. 1, 2019), https://www.hrw.org/sites/default/files/supporting_resources/hrw_ltr_to_doj.pdf [perma.cc/A89Z-ZZHA].

false or misleading forensic evidence.[51] For twenty years, FBI analysts gave flawed forensic testimony about microscopic hair comparisons, leading to at least thirty-two death sentences, of which fourteen have resulted in executions or deaths in prison.[52] Meanwhile, Massachusetts recently threw out thirty-one thousand criminal convictions and paid fourteen million dollars in settlement money in response to revelations about tainted and fraudulent drug forensic analyses.[53] Even DNA and fingerprint evidence have been shown to wrongfully convict.[54] These tragedies might never have been revealed, or others like them prevented, if the forensic methods had been secret.[55]

On the other hand, the policy rationale behind the law enforcement privilege is not frivolous. Some police investigative methods are potentially useless if would-be criminal actors know how they work.[56] Thus, the argument goes, some lawful, constitutional, and reliable investigative methods are so sensitive that disclosing them to criminal defense counsel or expert witnesses, even under a protective order, would pose untenable risks of leaks.[57] For instance, remote computer hacking tools that exploit vulnerabilities in computer systems can be used lawfully with a warrant and can prove crucial to investigating serious online crimes, such as the distribution of child sexual abuse materials,[58]

---

51. THE NATIONAL REGISTRY OF EXONERATIONS, https://www.law.umich.edu/special/exoneration/Pages/detaillist.aspx [perma.cc/JWU4-5QVH].

52. Spencer S. Hsu, *FBI Admits Flaws in Hair Analysis Over Decades*, WASH. POST (Apr. 18, 2015, 5:44 PM), https://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-matches-in-nearly-all-criminal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4-b510-962fcfabc310_story.html [perma.cc/6Q5W-MLW5].

53. Stephanie Barry, *Massachusetts Settles for $14 Million with 31,000 Criminal Defendants Whose Cases Were Tainted by Drug Lab Scandal*, MASSLIVE (June 2, 2022, 5:32 PM), https://www.masslive.com/news/2022/06/massachusetts-settles-for-14-million-with-more-than-31000-criminal-defendants-whose-cases-were-tainted-by-drug-lab-scandal.html [perma.cc/BZX7-8KTB].

54. Douglas Starr, *Forensics Gone Wrong: When DNA Snares the Innocent*, SCIENCE (Mar. 7, 2016), https://www.science.org/content/article/forensics-gone-wrong-when-dna-snares-innocent [perma.cc/2JV6-ZTF8]. *See generally* BRANDON L. GARRETT, AUTOPSY OF A CRIME LAB: EXPOSING THE FLAWS IN FORENSICS (2021).

55. *Cf.* Rediet Abebe et. al., *Adversarial Scrutiny of Evidentiary Statistical Software*, 2022 5TH ACM CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY, June 21–24, 2022, at 1733, https://doi.org/10.1145/3531146.3533228 (2022) (advocating criminal defense auditing of forensic software).

56. *E.g.*, United States v. Rigmaiden 844 F. Supp. 2d 982, 998 (D. Ariz. 2012); Tuite v. Henry, 181 F.R.D. 175, 176 (D.D.C. 1998). On counter-surveillance tactics, see Elizabeth E. Joh, *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, 55 ARIZ. L. REV. 997, 1005–11 (2013); Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 11–16 (2018); Bryan H. Choi, *A Prospect Theory of Privacy*, 51 IDAHO L. REV. 623 (2015); A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95, 155–59 (2017); Christopher S. Yoo & Arnav Jagasia, An Evidence-Based Lens on Privacy Values 35 (unpublished manuscript) (on file with *Michigan Law Review*).

57. *E.g.*, *In re* City of New York, 607 F.3d 923, 936–39 (2d Cir. 2010).

58. *See supra* notes 42–49 and accompanying text.

internet fraud,[59] and terrorism.[60] But if leaked, these tools instantly lose efficacy at scale. One such FBI hacking tool, which deanonymized computers visiting websites devoted to child sexual abuse material, was leaked to Reddit and, "within twelve hours," the vulnerability that it exploited was patched, rendering the tool useless.[61] Alternatively, leaked vulnerabilities that are not patched could be exploited by malicious actors to commit future crimes.[62] Having no privilege protections for those types of investigative methods could effectively prevent law enforcement from using them at all.[63]

The question of how courts should decide which privilege claims are valid is therefore a hard one. Should they rely on police testimony that secrecy is essential to the efficacy of an investigative technique? That testimony might be accurate, or it might be mistaken, exaggerated, pretextual, or fraudulent. Meanwhile, judges must evaluate privilege claims without the full adversarial process that they usually rely on to educate themselves about complex factual and legal issues. Instead, judges review allegedly privileged information in closed-door, *ex parte* proceedings, meaning only the law enforcement officers claiming privilege are present while defense counsel seeking the information are excluded. Such proceedings are valuable in that they avoid destroying a privilege in the process of determining its validity. However, they rob judges of the opportunity to hear additional facts and alternative viewpoints from the defense.[64] The absence of adversarialism, in turn, guts the checks and balances of criminal defense adjudication. It is virtually guaranteed to create bias favor-

59. *See, e.g.*, Zach Lerner, A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 YALE J.L. & TECH. 26, 34 (2016).

60. *See infra* notes 67–69 and accompanying text.

61. Nicholas Weaver, *The End of the NIT*, LAWFARE (Dec. 5, 2016, 2:30 PM), https://www.lawfaremedia.org/article/end-nit [perma.cc/9AMW-9EBL].

62. Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, LAWFARE (Jan. 13 2021, 8:57 AM), https://www.lawfaremedia.org/article/assessing-vulnerabilities-equities-process-three-years-after-vep-charter [perma.cc/U56X-Q62M].

63. One may question whether law enforcement *should* use hacking tools, but such methods are well established in current practice and illustrate one circumstance where the absence of any privilege protection might significantly impede lawful and constitutional investigations of serious crimes. *See generally* Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303 (2017); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570 (2018); Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014).

64. *See* JAMES E. PFANDER, CASES WITHOUT CONTROVERSIES 200–02 (2021).

ing law enforcement, and it encourages judges to give undue deference to police secrecy.[65] Indeed, judges sometimes just take police officers at their word and decline to look at the privileged information to check each claim.[66]

Related issues surrounding the state secrets privilege for national security and diplomatic information have inspired a robust literature.[67] Even important sub-issues have received sustained scholarly attention, such as precisely how much deference judges should afford to the government's national security claims[68] and whether public leaks of information vitiate the state secrets privilege.[69] In contrast, little is known and even less understood about

65. For a history and analysis of "structural spillover" that encourages judicial deference to police expertise, see Anna Lvovsky, *The Judicial Presumption of Police Expertise*, 130 HARV. L. REV. 1995, 2066 (2017). *See also* PFANDER, *supra* note 64, at 118–19; Shirin Sinnar, *Procedural Experimentation and National Security in the Courts*, 106 CALIF. L. REV. 991, 997–1001 (2018); Heidi Kitrosser, *Secrecy and Separated Powers: Executive Privilege Revisited*, 92 IOWA L. REV. 489, 504 (2007); Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. REV. 185 (2013).

66. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 599–600 (E.D. Va. 2016). *But see* Transcript of Motion Hearing at 17–18, United States v. Michaud, No. 15-cr-05351 (W.D. Wash. Feb. 17, 2016), ECF No. 162.

67. *See, e.g.*, Akbar, *supra* note 14; Aziz Z. Huq, *Structural Constitutionalism as Counterterrorism*, 100 CALIF. L. REV. 887 (2012).

68. *See* United States v. Reynolds, 345 U.S. 1, 11–12 (1953); Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081–82 (9th Cir. 2010); Robert Chesney, *No Appetite for Change: The Supreme Court Buttresses the State Secrets Privilege, Twice*, 136 HARV. L. REV. 170, 178 (2022) [hereinafter *No Appetite*]; Sinnar, *supra* note 65, at 999–1006; Huq, *supra* note 67; Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361 (2009); Michael H. Page, Note, *Judging Without the Facts: A Schematic for Reviewing State Secrets Privilege Claims*, 93 CORNELL L. REV. 1243, 1275–83 (2008); David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 653, 676 (2005).

69. *See* United States v. Zubaydah, 142 S. Ct. 959, 969–72 (2022); JENNIFER K. ELSEA & EDWARD C. LIU, CONG. RSCH. SERV., R47081, THE STATE SECRETS PRIVILEGE: NATIONAL SECURITY INFORMATION IN CIVIL LITIGATION 13, 19 (2022); Anthony John Trenga, *What Judges Say and Do in Deciding National Security Cases: The Example of the State Secrets Privilege*, HARV. NAT'L SEC. J. 20–21 (2018), https://harvardnsj.org/wp-content/uploads/2018/01/1_Trenga_StateSecrets.pdf [perma.cc/W94A-Q6PG]; TODD GARVEY & EDWARD C. LIU, CONG. RSCH. SERV., R41741, THE STATE SECRETS PRIVILEGE: PREVENTING THE DISCLOSURE OF SENSITIVE NATIONAL SECURITY INFORMATION DURING CIVIL LITIGATION 11–12 (2011); Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 91–139 (2010); Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1293–96 (2007); Note, *The Military and State Secrets Privilege: Protection for the National Security or Immunity for the Executive?*, 91 YALE L.J. 570, 580 (1982).

the domestic law enforcement privilege, which differs from the national security context in crucial respects.[70] Prior scholarship on the subject is sparse.[71] Leading evidence law treatises mention it only in passing.[72] And courts have developed ambiguous and incoherent doctrine around asserting and evaluating claims to the privilege.[73]

This Article aims to fill that gap in the literature. It uses primary sources that include eighteenth-century trial transcripts, twenty-first-century PACER filings, and police-vendor contracts recently released to the public. Part I explains the equities on both sides of the privilege. Part II details how the privilege currently works in practice, culminating in a critique that the requirements for asserting a threshold claim to the privilege are so vague as to be effectively meaningless.

Part III turns from positive to normative. It offers a skeptical account of existing arguments against the privilege, drawing from litigation documents and the small amount of prior scholarship on the topic. It begins by debunking the current scholarly consensus that there was no privilege for law enforcement methods at common law. That view is almost certainly wrong and invites a naïve underestimation of the privilege's intractability. Next, Part III considers prior arguments that the privilege should be abolished entirely or should not apply to information possessed by private entities. While these arguments may well rally a pro-transparency community around a shared set of beliefs, they have important limitations and are unlikely to satisfy skeptics.

Part IV proposes an alternative to reasonably constrain the privilege with minimal risk to law enforcement efficacy: Tie secrecy claims to law enforcement's own pre-dispute conduct. There should be two steps to this analysis. *First*, regarding the threshold question of whether a privilege invocation is ap-

---

70. Differences include the likelihood that law enforcement will seek to introduce the results of secret investigative methods in court, *cf.* Akbar, *supra* note 14, at 850–51, and courts' willingness to undertake *in camera* review. *Cf. Reynolds*, 345 U.S. at 10–11. However, the line between military secrecy and domestic police secrecy is complicated by the racialized history of militarizing civilian police. *See* Fanna Gamal, Note, *The Racial Politics of Protection: A Critical Race Examination of Police Militarization*, 104 CALIF. L. REV. 979, 1005–06 (2016).

71. The most extensive article on the privilege examines its history and argues that it should not exist. *See* Stephen Wm. Smith, *Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233, 269–75 (2017). Two more articles include brief discussions of the privilege in the context of broader arguments about police secrecy exemptions to public records laws. *See* Koningisor, *supra* note 13, at 652–54; Manes, *supra* note 13, at 552–57. Meanwhile, two student notes have argued to enhance the secrecy power that the privilege affords. *See* Rupinder K. Garcha, Note, *Nits a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases*, 93 N.Y.U. L. REV. 822, 857–60 (2018); Charles M. Bell, Note, *Surveillance Technology and Graymail in Domestic Criminal Prosecutions*, 16 GEO. J.L. & PUB. POL'Y 537, 557–58 (2018). CIPA increases secrecy by permitting the prosecution to disclose redacted versions or summaries of classified information in lieu of actual evidence. 18 U.S.C. app. § 4.

72. *See, e.g.*, 26A CHARLES ALAN WRIGHT, KENNETH W. GRAHAM, JR. & ANN MURPHY, FEDERAL PRACTICE AND PROCEDURE: EVIDENCE § 5681 (1992 & Supp. 2024).

73. *See infra* text accompanying notes 156–187.

propriate at all, judges should demand to know the conditions that law enforcement itself previously imposed on access to the putatively secret information. The answer to that question can be adjudicated publicly without jeopardizing a legitimate privilege claim and will serve as a signal for the value of secrecy. If law enforcement has not taken sufficient care with the information, courts should default to denying privilege. *Second*, even when the government can cross the initial threshold by showing reasonable care, it should still be possible in many cases to accommodate defense access. Here is how: If a court-ordered protective order can match or exceed the safeguards that law enforcement itself has previously maintained, judges should again default to ordering disclosure.

This approach sets out a basic floor for transparency: The privilege should not afford greater secrecy within the courts than law enforcement has imposed outside them. While this proposal might seem obvious once articulated, it is a far cry from existing doctrine. Courts rarely inquire into the conditions of prior dissemination. More broadly, in developing this proposal, this Article articulates a general theory of confidentiality's role in privilege law as a whole.

The law enforcement privilege offers valuable safeguards for effective, lawful, and constitutional investigative methods. At the same time, it invites overclaiming and abuse; empowers police to conceal misconduct and evade accountability; and undermines the truth-seeking process of the courts. A privilege that risky should have clear constraints in law. In the memorable words of Judge Learned Hand writing about a case in which the FBI sought to conceal records of illegal wiretapping:

> Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which it seeks to forfeit the liberty of its citizens . . . . A society which has come to wince at such exposure of the methods by which it seeks to impose its will upon its members, has already lost the feel of freedom and is on the path towards absolutism.[74]

I. THE ACCESS VERSUS SECRECY CONUNDRUM

For nearly a decade, the Orange County Sheriff's Department ran an unconstitutional jailhouse informant program.[75] In a recent report exposing it, the United States Department of Justice described how law enforcement maintained a vast, secretive system "to track, manage, and reward" the informants,[76] while concealing exculpatory information about them from the defendants

74. United States v. Coplon, 185 F.2d 629, 638 (2d Cir. 1950).

75. Press Release, Off. of Pub. Affs., U.S. Dep't of Just., Justice Department Finds Civil Rights Violations by Orange County, California, District Attorney's Office and Sheriff's Department in Use of Jailhouse Informants (Oct. 13, 2022), https://www.justice.gov/archives/opa/pr/justice-department-finds-civil-rights-violations-orange-county-california-district-attorney-s [perma.cc/ZPW6-HKY9].

76. *Id.*

they were informing against.[77] The Department of Justice concluded that hiding the program from criminal defendants enabled it to "operate so widely and for so long."[78] As the Orange County abuses show, secrecy breeds impunity. Without disclosures to facilitate meaningful judicial review, illegal and unconstitutional police practices can flourish indefinitely.

The law enforcement privilege is not the only way police conceal illegal methods, but it may be the least costly for them. Police do not need a special secrecy power if they never introduce the results of secret investigative methods in court. Alternately, they can conceal their methods through "parallel construction," a constitutionally suspect tactic of conducting a second, transparent investigation to rediscover evidence in a judicially palatable form.[79] Those techniques at least impose some cost on police that can curtail their adoption.

Not so with the law enforcement privilege, which empowers police and prosecutors to keep investigative methods secret *while introducing* the results of those methods in court. No evidence need be foresworn, nor duplicate investigation conducted.

It is difficult to quantify the scale of privilege invocations due to the inaccessibility of trial court records (which are not generally included in major legal research databases), as well as variations in terminology between jurisdictions. Nonetheless, some metrics are available. Over the past roughly forty years, federal courts have used the labels "law enforcement privilege," "law enforcement evidentiary privilege," or "law enforcement investigatory privilege" in more than eleven hundred opinions.[80] State courts have done so less than one hundred times,[81] but many state courts protect similar information using alternate privilege names, such as the "official information privilege"[82] or by analogy to the confidential informant privilege.[83] Meanwhile, the software at

77. CIV. RTS. DIV., U.S. DEP'T OF JUST., INVESTIGATION OF THE ORANGE COUNTY DISTRICT ATTORNEY'S OFFICE AND THE ORANGE COUNTY SHERIFF'S DEPARTMENT 60 (2022), https://www.justice.gov/media/1251036/dl%20 [perma.cc/F4EX-5EK6].

78. *Id.*

79. HUM. RTS. WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN U.S. CRIMINAL CASES (2018).

80. Search Results: Federal and State Court Opinions Mentioning Law Enforcement Privilege, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Apr. 13, 2023) (search "adv: 'law enforcement privilege' OR 'law enforcement evidentiary privilege' OR 'law enforcement investigatory privilege' ").

81. *Id.* (showing, as of April 23, 2023, eighty-five state cases).

82. *E.g.*, State v. Garcia, 618 A.2d 326, 328 (N.J. 1993) (applying the "official information privilege" to surveillance locations); *accord* People v. Moreno, No. B235421, 2013 WL 97317, at *7 (Cal. Ct. App. Jan. 9, 2013) (applying a California state evidence code provision that "provides a privilege against public disclosure of 'official information.' "); People v. Montgomery, 252 Cal. Rptr. 779, 782–84 (Ct. App. 1988) ("A public entity has the privilege of refusing to disclose and of preventing another from disclosing official information . . . .").

83. *See, e.g.*, People v. Palmer, 92 N.E.3d 483, 490–91 (Ill. App. Ct. 2017) (recognizing a "surveillance location privilege" derived from the confidential informant's privilege); United

issue in *United States v. Pirosko* has been cited in at least eighty-nine criminal cases,[84] similar internet investigative software programs have been cited in at least sixty-four criminal cases,[85] and password-cracking data extraction tools that also trigger law enforcement privilege claims[86] have been cited in over six hundred criminal cases.[87] These numbers almost certainly vastly understate the number of times the privilege has successfully concealed police conduct in discovery disputes that did not lead to written opinions.

This Part examines the policies and procedures behind this secrecy power. It describes circumstances in which criminal defendants have compelling interests in accessing information about law enforcement methods, the procedures available to obtain it, and the risks that those procedures may be abused. That is followed by an account of circumstances in which law enforcement has compelling interests in keeping investigative methods secret, the evidentiary privilege procedures available to maintain that secrecy, and the risks that those procedures may be abused. In the words of one federal judge, "What should be done about it when, under these facts, the defense has a justifiable need for information in the hands of the government, but the government has a justifiable right not to turn the information over to the defense?"[88]

A. *Criminal Defense Interests in Access*

Criminal defendants can have an array of interests in scrutinizing law enforcement methods. To start, they can have a strong interest in discovering

States v. Green, 670 F.2d 1148, 1150 (D.C. Cir. 1981) (holding that the District Court correctly recognized the Government's "qualified privilege" to keep confidential its surveillance locations).

84. United States v. Pirosko, 787 F.3d 358, 363 (6th Cir. 2015); Search Results: +Shareaza, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Aug. 1, 2023) (search "+Shareaza").

85. Search Results: +EP2P, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Aug. 1, 2023) (search "+EP2P") (showing 29 results); Search Results: Child Protection Systems and CPS, Westlaw, https://1.next.westlaw.com/Search/Home.html (last visited Aug. 1, 2023) (search "adv: 'Child Protection! System' & CPS") (showing 35 results).

86. *See, e.g.*, United States v. Daniels, 652 F. Supp. 3d 1191, 1193–94 (S.D. Cal. 2023); Thomas Reed, *GrayKey iPhone Unlocker Poses Serious Security Concerns*, MALWAREBYTESLABS (Mar. 15, 2018) https://www.malwarebytes.com/blog/news/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns [perma.cc/32NZ-AB4K].

87. Search Results: Cellebrite, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Mar. 23, 2025) (search "Cellebrite" cases and filter "Criminal") (showing over 600 results); Search Results: GrayKey, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Mar. 23, 2025) (search "GrayKey" cases and filter "Criminal") (showing at least 50 results).

88. Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 5, United States v. Michaud, No. 15-cr-5351 (W.D. Wash. May 18, 2016), ECF No. 205.

information about methods used to establish probable cause for a search warrant.[89] In the case of investigative technologies, defendants may seek information about both functional characteristics and reliability.[90] They may seek to argue that the outputs are biased based on race or other constitutionally protected characteristics,[91] or are otherwise insufficiently reliable to establish probable cause.[92] They may seek to argue that, as with Stingrays, the functional characteristics mean that use of the technology constitutes a Fourth Amendment search or seizure.[93] They may seek a hearing to determine whether law enforcement officers lied about the technology in a warrant application.[94] In the context of facial recognition software in particular, defendants may seek to argue that use of the software constituted an unreliable[95] or unduly suggestive[96] identification procedure in violation of due process. Each of these arguments can support a motion to suppress.[97]

Similar issues arise when the prosecution relies on the results of surveillance or forensic technologies as evidence of guilt. This happens even with

89. *See, e.g.*, United States v. Norris, 942 F.3d 902, 909–10 (9th Cir. 2019); United States v. Stanley, 753 F.3d 114, 123–24 (3d Cir. 2014). Police in both cases used MoocherHunter, a "low-profile/covert-tracking" software, to gather evidence to establish probable cause. *MoocherHunter Law Enforcement Edition*, THINK SECURE, https://securitystartshere.org/page-software-moocherhunter.htm#moocherhunterlawenforcementedition [perma.cc/AL5T-L4YK].

90. *See* New Jersey v. Arteaga, 296 A.3d 542, 546 (N.J Super. Ct. App. Div. 2023).

91. *See, e.g.*, Commonwealth v. Dilworth, 147 N.E.3d 445 (Mass. 2020) (denying law enforcement privilege claim for information about undercover Snapchat accounts, which a criminal defendant sought for purposes of proving a claim of racially biased selective enforcement in violation of the equal protection standard). As another example, biometric surveillance software such as face recognition can have disparate accuracy rates based on race, gender, and age. *E.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77 (2018). Machine learning software trained with carceral data sources can reproduce the biases built into past carceral practices. Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. 2007 (2022). *But see* Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1271–77 (2017). At the same time, even if surveillance software does not rely on racially biased algorithms, police may deploy the software to disproportionately surveil racial minorities and other historically marginalized groups. Indeed, the United States has a long history of law enforcement surveillance disproportionately deployed against racial minorities. *See generally*, Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043 (2018); Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54 (2019).

92. *C.f.* Florida v. Harris, 568 U.S. 237, 245–49 (2013). For a recent argument regarding the reliability standard that should apply to investigative technologies used to establish probable cause, see Amici Curiae Brief of Pa. Innocence Project, et al. in Support of Appellant Jamar Foster, Commonwealth v. Foster, No. 12 WAP 2024 (Pa. July 5, 2024).

93. *See generally*, Mayer, *supra* note 63.

94. *See* Franks v. Delaware, 438 U.S. 154 (1978).

95. *See* Manson v. Brathwaite, 432 U.S. 98 (1977).

96. *See* Commonwealth v. Johnson, 650 N.E.2d 1257 (Mass. 1995); People v. Adams, 423 N.E.2d 379 (N.Y. 1981).

97. *See* State v. Arteaga, 296 A.3d 542 (N.J. Super. Ct. App. Div. 2023).

technologies that police generally use solely for investigative leads.[98] For instance, consider police use of internet monitoring software to identify computers that appear to be sharing digital contraband. Police may rely on the outputs of that software to establish probable cause to obtain a warrant and then use the warrant to conduct a physical search of a suspect's home and computer. If police find contraband during the search, the prosecution can charge the defendant with *possession*. But the initial results generated by the surveillance software may be the sole evidence supporting a charge of *distribution* at trial.[99] When the outputs of surveillance software could be introduced as direct evidence at trial, defendants may seek to challenge the reliability of the software system in a *Daubert* or *Frye* admissibility hearing. Alternately, defendants may seek information about the reliability or functional characteristics of the software to prepare for cross-examination at trial.[100] Or perhaps knowing how the software functions could help to identify evidence of innocence, such as a recurring query that initially identifies contraband and then shortly thereafter provides a null result indicating rapid deletion and tending to negate *mens rea*. Whether for an admissibility challenge, cross-examination, or evidence of innocence, accessing information about how, and how well, an investigative or forensic technology works can be essential to provide an effective defense.[101] In all of these circumstances, defendants' rights to access, scrutinize, and contest the evidence against them are essential to reduce wrongful convictions, serve dignitary and legitimacy interests in criminal proceedings, surface unconstitutional or unlawful surveillance practices, and more generally facilitate judicial review of law enforcement conduct.[102]

Notably, there is also a risk that criminal defense counsel might strategically demand access to sensitive information about law enforcement methods in a ploy to raise the costs of pursuing the case and "graymail" the prosecution into dropping criminal charges.[103] Concern that defense counsel might undertake a graymail strategy seeking access to *classified* information led Congress to enact the Classified Information Procedures Act (CIPA).[104] CIPA Section 4

98. The boundary between surveillance, investigative, and forensic methods is blurry. When the results of a method are introduced as evidence of guilt, the use becomes forensic. *See* Ferguson, *supra* note 41, at 837.

99. *See, e.g.*, Motion to Compel Discovery at 9, United States v. Clements, No. 15-cr-00275 (N.D. Ohio Jan. 18, 2016), ECF No. 17.

100. *See, e.g.*, Defendant's Response to the Government's Motion in Limine at 3–4, United States v. Chiaradio, No. 09-cr-00069 (D.R.I. Oct. 19, 2010), ECF No. 74.

101. *Cf.* State v. Pickett, 246 A.3d 279, 298–99 (N.J. Super. Ct. App. Div. 2021).

102. *Cf.* Cynthia H. Conti-Cook, *Defending the Public: Police Accountability in the Courtroom*, 46 SETON HALL L. REV. 1063, 1074–78 (2016); Erik Luna, *Transparent Policing*, 85 IOWA L. REV. 1107, 1123 (2000).

103. Bell, *supra* note 70.

104. Steven Aftergood, *A Tutorial on the Classified Information Procedures Act*, FED'N OF AM. SCIENTISTS (May 10, 2010), https://www.fas.org/publication/cipa_tutorial [perma.cc/63FD-BTQ7]; *see* 18 U.S.C. app. §§ 1–16.

gives judges discretion to authorize redactions or substitutions of classified information and entitles the government to argue for those redactions or substitutions in a closed-door, *ex parte* hearing.[105] Analogous concerns over graymail can arise with all sorts of sensitive information. However, outside the classified-information context, no special CIPA-like statute addresses these concerns.

Instead, a combination of baseline criminal procedure rules and privilege law mitigate the graymail risk. The baseline criminal procedure rules do so in part by placing strict limits on defendants' affirmative rights to compel access to information. Importantly, defendants cannot compel access to *irrelevant* information. Criminal discovery rules require defendants to show that any documents or data they seek from the government are "material to preparing the defense,"[106] meaning the information has "more than . . . some abstract logical relationship to the issues in the case" and would enable them "significantly to alter the quantum of proof in [their] favor."[107] Criminal subpoenas require defendants to identify information with specificity and to establish in advance that the information is likely to be both relevant and admissible at trial.[108] And judges have broad discretion to deny harassing or frivolous discovery motions.[109] If these rules function correctly, defendants will only ever be able to compel access to information about law enforcement investigative methods that is likely to be relevant to their case—even if no privilege applies.

Further, beyond the baseline relevance requirements and prohibitions on frivolous motions and fishing expeditions, the strength of defendants' rights to compel access to evidence also varies considerably based on the type of motion they are making and the stage of proceeding. Defendants' confrontation and compulsory process rights reach their zenith at trial. So, if a defendant can show a need for information at trial, then courts are more likely to prioritize the defendant's rights over countervailing secrecy interests (to, for instance, pierce any conflicting evidentiary privileges).[110] In contrast, defendants' compulsory process rights are generally weaker pretrial[111]—a consequential distinction given that over ninety percent of criminal defendants plead guilty pretrial.[112] Hence, a defendant's pretrial subpoena may fail to defeat a conflicting secrecy interest (or pierce a conflicting evidentiary privilege) even if a trial

105. 18 U.S.C. app. § 4.

106. FED. R. CRIM. P. 16(a)(1)(E); FED. R. CRIM. P. 16 advisory committee's note to 1966 amend.

107. United States v. Ross, 511 F.2d 757, 762–63 (5th Cir. 1975).

108. *See* United States v. Nixon, 418 U.S. 683, 699–700 (1974).

109. *See* FED. R. CRIM. P. 16 advisory committee's note to 1966 amendment; *Nixon*, 418 U.S. at 699–700.

110. *See, e.g.*, United States v. Budziak, 697 F.3d 1105, 1111–13 (9th Cir. 2012).

111. *See, e.g.*, Pennsylvania v. Ritchie, 480 U.S. 39, 52 (1987).

112. *Criminal Cases*, U.S. CTS., https://www.uscourts.gov/about-federal-courts/types-cases/criminal-cases [perma.cc/Z69M-DWMY].

subpoena would do so.[113] The strength of a defendant's access interests will also, of course, be fact specific. For surveillance and investigative software in particular, a defendant's ability to persuade a court that they have a legitimate interest in access may depend on the precise information that a defendant seeks about the software and whether the results generated by law enforcement's use of that software can be verified without using software.[114]

Finally, for certain limited categories of information deemed especially sensitive, privilege law provides additional protections against disclosure, and thereby against graymail as well. These heightened protections impose well-recognized costs on the accuracy and fairness of adjudicatory outcomes because they necessarily suppress *relevant* evidence from the opposing party, judge, and jury alike. In the Supreme Court's oft-repeated words, privileges "are in derogation of the search for truth."[115] Privilege law attempts to balance those costs against the benefits that privileges supposedly provide for social policies that are extrinsic to the truth-seeking function of the courts. The following Section discusses the putative societal benefits of law enforcement privilege claims.

B. *Law Enforcement Interests in Secrecy*

The law enforcement privilege is grounded in the policy rationale that some investigative methods would become ineffective if details about how they work were generally known.[116] There are high-tech and low-tech examples. If everyone knew the algorithm for software that detects known child sexual abuse materials online, it would be easier for those trafficking in such materials to slightly alter the files and avoid detection.[117] If everyone knew the location of secret serial numbers on vehicles, it would be easier for people stealing cars to tamper with that evidence.[118] If everyone knew the range and location of an audio bug, it would be easier for people to go talk somewhere else. If everyone had access to facial recognition and voice print algorithms, they could develop adversarial machine learning attacks to fool the systems and

113. *See, e.g.*, People v. Hammon, 938 P.2d 986 (Cal. 1997).

114. *See* Steven M. Bellovin, Matt Blaze, Susan Landau & Brian Owsley, *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO STATE TECH. L.J. 1, 64–66 (2021).

115. United States v. Nixon, 418 U.S. 683, 710 (1974).

116. *E.g.*, United States v. Rigmaiden, 844 F. Supp. 2d 982, 999 (D. Ariz. 2012); Tuite v. Henry, 181 F.R.D. 175, 176 (D.D.C. 1998); Bambauer & Zarsky, *supra* note 56, at 16–17.

117. Michael H. Keller & Gabriel J.X. Dance, *Child Abusers Run Rampant as Tech Companies Look the Other Way*, N.Y. TIMES (Nov. 9, 2019), https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html [perma.cc/7WVJ-HE9J].

118. *See* People v. Moreno, No. B235421, 2013 WL 97317, at *7 (Cal. Ct. App. Jan. 9, 2013); People v. Marghzar, 239 Cal. Rptr. 130, 132 (Cal. Ct. App. 1987); *In re* David W., 133 Cal. Rptr. 342, 346 (Cal. Ct. App. 1976).

avoid identification.[119] Indeed, now that knowledge of Stingrays has grown more widespread, both Google and Apple have developed optional user settings to block cell-site simulators from connecting to their phones, which presumably makes it easier for those committing crimes (and everyone else) to use their cell phones while avoiding Stingray tracking.[120]

Crucially, the law enforcement privilege presumes that the protected information is so sensitive that it cannot be disclosed to defense counsel or expert witnesses, even under a strict protective order.[121] This rationale can be taken to the extreme. Multiple courts have upheld a law enforcement privilege claim to withhold information from a defense expert witness.[122] The risk of abuse or misuse is obvious. Police and prosecutors might lie, exaggerate, or make a mistake about the importance of secrecy to the efficacy of an investigative method. They might overclaim the privilege due to a general culture of secrecy[123] or out of an institutional interest in avoiding adversarial scrutiny.[124] Or they might claim the privilege pretextually to willfully conceal negligent, unconstitutional, or even criminal conduct.

This latter possibility is hardly remote. History is replete with examples of law enforcement officers lying about their investigative sources and methods.[125] In 2000, the Department of Justice admitted to a series of "misstatements and omissions of material facts" in applications for FISA warrants.[126] In 1997, Montgomery police were found to have falsified the identity of informants and "recorded informant money as being transferred to non-existent informants, presumably pocketing the money themselves."[127] In 1989, Boston police admitted to falsifying a nonexistent informant.[128] And in 1969, when

---

119. Patrick O'Reilly, Andreas Bugler, Keshav Bhandari, Max Morrison & Bryan Pardo, *VoiceBlock: Privacy Through Real-Time Adversarial Attacks with Audio-to-Audio Models*, *in* 35 ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS (2022).

120. *See* Cooper Quintin, *Apple and Google Are Introducing New Ways to Defeat Cell Site Simulators, But Is it Enough?*, ELECTRONIC FRONTIER FOUND. (Sept. 13, 2023), https://www.eff.org/deeplinks/2023/09/apple-and-google-are-introducing-new-ways-defeat-cell-site-simulators-it-enough [perma.cc/M87Y-MN6R]; *see also Anti Spy Detector - Spyware*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.protectstar.antispy.android&hl=en_US&pli=1 [perma.cc/B2M8-H7CU].

121. *See, e.g.*, *In re* City of New York, 607 F.3d 923, 936–39, 935 n.12 (2d Cir. 2010).

122. *See* United States v. Tippens, No. CR16-5110, 2017 WL 11511726, at *2 (W.D. Wash. Mar. 16, 2017); *see also* United States v. Budziak, No. 08-CR-00284, 2009 WL 1392197, at *1–2 (N.D. Cal. May 14, 2009) (order denying motion to compel).

123. *See* Friedman, *supra* note 34, at 118.

124. *See* Anna Lvovsky, *Rethinking Police Expertise*, 131 YALE L.J. 475, 553 (2021).

125. *See* Stephen W. Gard, *Bearing False Witness: Perjured Affidavits and the Fourth Amendment*, 41 SUFFOLK U.L. REV. 445, 447–52 (2008); *see, e.g.*, Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1038, 1041 (1996).

126. *In re* All Matters Submitted to Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, 620 (FISA Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

127. Riley v. City of Montgomery, 104 F.3d 1247, 1250 (11th Cir. 1997).

128. Commonwealth v. Lewis, 542 N.E.2d 275, 275 (Mass. 1989).

fourteen heavily armed Chicago police officers broke into an apartment to assassinate Black Panther leader Fred Hampton,[129] they used a warrant based on a perjured affidavit about a confidential informant who did not exist.[130]

Given this history, the basic worry is that the law enforcement privilege will be used to conceal too much. For instance, courts have declined to categorically refute claims that the privilege shields the type of batteries used in an audio recording device,[131] or "the charts, graphs, and raw data" generated during a polygraph examination.[132] Shielding this type of information from adversarial scrutiny can enable tragic misconduct. Consider that, in July 2023, the Third Circuit found sufficient evidence for a jury to conclude that a detective fabricated polygraph evidence, which led to an innocent man's wrongful eleven-year prison sentence.[133] A privilege sweeping enough to encompass polygraph data can prevent that type of misconduct from ever coming to light. Yet critics have complained that courts "apply the privilege broadly to prohibit disclosure of information about all manner of technology, even techniques that are decades old and well known to anyone who has ever watched a police procedural,"[134] and that judges accept claims to the privilege at face value without demanding robust proof that disclosing an investigative method would in fact entail a risk of evasion.[135]

While the Stingray saga described above is arguably the flagship narrative of abuse for the domestic law enforcement privilege, it is hardly the only example. Consider *United States v. Budziak*,[136] one of the rare federal appellate opinions rejecting a law enforcement privilege claim for information about an internet monitoring software system.[137] The Ninth Circuit opinion in *Budziak* has been cited over four hundred times since its publication in 2012.[138] Criminal defendants seeking access to information about internet surveillance, remote computer access, and government hacking tools frequently rely on

129. Hampton v. Hanrahan, 600 F.2d 600, 605, 612 (7th Cir. 1979).

130. *Id.* at 637–38.

131. *See, e.g.*, United States v. Farha, No. 11-CR-115-T-30, 2012 WL 12964913, at *3 (M.D. Fla. Sept. 27, 2012).

132. Shah v. Dep't of Just., 714 Fed. App'x. 657, 658 (9th Cir. 2017).

133. Mervilus v. Union County, 73 F.4th 185, 192, 195 (3d Cir. 2023).

134. Manes, *supra* note 13, at 553.

135. Jonathan Manes has argued that courts evaluating law enforcement privilege claims "often require little if any demonstration that disclosure of the information sought would create a significant risk of circumvention." *Id.* at 554. And Margaret Kwoka has made similar arguments regarding national security secrecy in FOIA. Kwoka, *supra* note 65, at 221–35.

136. United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).

137. *Id.* at 1112.

138. Search Results: "697 F.3d 1105" Citing References, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Apr. 16, 2025) (search "697 F.3d 1105"; then select "citing references").

Budziak's reasoning about the materiality of such information to their defense.[139] Many judicial opinions go to substantial lengths to distinguish *Budziak* before denying defense discovery motions.[140] Despite the centrality of the case, courts and commentators have overlooked key facts in *Budziak* that illustrate why it is so harmful when judges rubber stamp privilege claims.

In *Budziak*, the FBI used a remote computer access software program to investigate contraband on the defendant's computer.[141] The defense sought access to an executable copy, technical specifications, and documentation for the software[142] for purposes of a Fourth Amendment suppression motion.[143] The prosecution asserted the law enforcement privilege, arguing that the software was "created by the FBI and used exclusively for law enforcement purposes,"[144] and that disclosure "would reveal confidential features of the software"[145] that would help criminal actors "to frustrate the FBI's ability to detect them . . . [and] jeopardize ongoing and future investigations."[146] Nonetheless, the Ninth Circuit held that the defendant was entitled to discover the information,[147] and, on remand, the district court ordered disclosure not merely of the executable software but also of the program's source code, subject to a protective order.[148]

Two months later, the FBI admitted that it did not have the source code and did not know where it was.[149] At this point, the prosecution revealed that the software was not actually created "by the FBI,"[150] but rather by a private

139. In *Budziak*, the Ninth Circuit reasoned that "criminal defendants should not have to rely solely on the government's word that . . . discovery is unnecessary." *Budziak*, 697 F.3d at 1113.

140. *See, e.g.*, United States v. Harney, No. 16-38-DLB-CJS, 2018 WL 1145957 (E.D. Ky. Mar. 1, 2018), *aff'd*, 934 F.3d 502 (6th Cir. 2019) (distinguishing the defendant's case from Budziak for seemingly-trivial differences in the parties' discovery requests).

141. *Budziak*, 697 F.3d at 1107.

142. Defendant's Reply on Remand to United States' Memorandum RE Discovery Issues at 4–5, United States v. Budziak, No. 08-CR-00284 (N.D. Cal. Oct. 24, 2013), ECF No. 234.

143. Notice of Motion and Motion to Compel Discovery Pursuant to Rule 16(a)(1)(E) and *Brady* at 2–3, *Budziak*, No. 08-CR-00284 (Dec. 13, 2010), ECF No. 115.

144. United States' Opposition to Defendant's Third Motion to Compel Discovery, to Defendant's Second Motion to Suppress, and to Defendant's Request for an Evidentiary Hearing at 7, 13, *Budziak*, No. 08-CR-00284 (Dec. 16, 2010), ECF No. 123 [hereinafter Opposition to Defendant's Third Motion].

145. United States' Supplemental Opposition to Defendant's Third Motion to Compel Discovery, to Defendant's Second Motion to Suppress, and to Defendant's Request for an Evidentiary Hearing at 2, *Budziak*, No. 08-CR-00284 (Dec. 27, 2010), ECF No. 127.

146. *Id.* at 6.

147. United States v. Budziak, 697 F.3d 1105, 1112 (9th Cir. 2012).

148. United States v. Budziak, 08-CR-00284 (N.D. Cal. Feb. 18, 2014) (Protective Order re: Defendant Access to eP2P Software Program), ECF No. 248.

149. Defendant Budziak's Status Memorandum re: Inspection of Gov't Software at 2, *Budziak*, No. 08-CR-00284 (Apr. 24, 2014), ECF No. 249.

150. Opposition to Defendant's Third Motion, *supra* note 144, at 7.

contractor.[151] Moreover, the contractor's employees had since dispersed, and the FBI did not know whether any of them possessed copies of the information.[152] The prosecution's inability to comply with the court's disclosure order ultimately led to a dismissal of criminal charges in the case.[153] Beyond failing to archive its own copy of the code, the FBI appears to have handled an allegedly sensitive investigative method with remarkably lax security by failing to keep track of code copies in the hands of its contractor and the contractor's departing employees. If *Budziak* had followed the far more common pattern of courts upholding law enforcement privilege claims, this negligent treatment of the source code might never have come to light. A routine requirement for law enforcement to disclose the safeguards it has imposed on allegedly privileged information could expose negligent conduct and rightly incentivize the government to take greater care with truly sensitive information.

* * *

This Part initially situated the law enforcement privilege in the broader context of criminal defendants' interests in accessing covered information, the procedures for doing so, and the risks of abuse that those procedures create. It then explained the reasons for affording law enforcement some measure of secrecy in this arena, the procedures for doing so, and the risk that those procedures could be abused. The following Parts describe and critique both the existing procedures for asserting the privilege and the most common existing proposals for limiting its abuse.

II. DOCTRINE AND DISCONTENTS

The specter of police secrecy and its authoritarian undertones takes on distinct urgency as the nation struggles to reckon with violence, abuse, and systemic racism in policing. Raising the stakes further still, new technologies—from taser-equipped persistent surveillance drones to social media monitoring software, facial recognition algorithms, and the pervasive use of license plate readers[154]—threaten to entrench and automate the harms of unequitable and unaccountable policing. Given this context, the law enforcement privilege and *Pirosko* line of cases denying criminal defendants "access to confidential

151. United States' Response to Defendant's Motion for Discovery Remedy at 4, *Budziak*, No. 08-CR-00284 (May 1, 2014), ECF No. 251.

152. *Id.*

153. United States v. Budziak, No. 08-CR-00284 (N.D. Cal. June 5, 2014) (criminal minute order), ECF No. 255; United States' Response to Defendant's Motion for Discovery Remedy, *supra* note 151, at 2.

154. Barry Friedman, Wael Abd-Almageed, Miles Brundage, Ryan Calo, Danielle Citron, Rebekah Delsol, Chris Harris, Jennifer Lynch & Mecole McBride, *Statement of Resigning Axon AI Ethics Board Members*, POLICING PROJECT (June 6, 2022), https://www.policingproject.org/statement-of-resigning-axon-ai-ethics-board-members [perma.cc/GNF5-KF79].

government investigative software"[155] will no doubt influence the terms of secrecy for a far broader array of police technologies.

This Part describes existing law enforcement privilege doctrine and argues that its requirements for asserting threshold claims to the privilege are so vague as to be practically meaningless. They boil down to a restatement of the privilege's underlying policy rationale: Disclosure could render an investigative method less effective. Yet, taken to its logical extreme, few, if any, investigative methods would not qualify for protection under this rationale. The result is an effectively boundless police secrecy power.

A. *Current Law Enforcement Privilege Doctrine*

In broad strokes, current law enforcement privilege doctrine requires a two-step inquiry. The first step assesses whether law enforcement has established a threshold claim to the privilege. If yes, then the second step requires balancing law enforcement's interest in secrecy against the defendant's interest in accessing the information.[156]

Beyond this basic outline, however, the doctrine offers few details about how the privilege should function. Unlike the related state secrets, official information, and confidential informant privileges, the draft Federal Rules of Evidence lacked a distinct law enforcement privilege by that name; so, the legislative history and advisory committee notes for the rules contain few definitive clues.[157] The Supreme Court has never spoken to the contours of the law enforcement privilege, or even to its existence.[158] And appellate authorities recognizing it are vague, leaving trial courts with minimal guidance and maximal discretion. At one extreme, the Ninth Circuit has refused to weigh in at all. It asserted in 2017 that it has "yet to recognize or reject" a "law enforcement privilege that covers law enforcement techniques and procedures,"[159] leaving

155. United States v. Gonzales, No. CR-17-01311-001-PHX, 2019 WL 669813, at *3 (D. Ariz. 2019).

156. Tuite v. Henry, 98 F.3d 1411, 1413, 1416–19 (D.C. Cir. 1996). As with all evidentiary privileges, there is a separate and distinct conflict between secrecy interests and the public's right of access to the courts. Again, as with all privileges, that conflict is resolved at a later stage with another different balancing test for weighing the First Amendment and common-law public rights of access to the courts. *See* discussion *infra* Section IV.C.3.

157. *Cf.* FED. R. EVID. 509–10 advisory committee's notes to amends. (not enacted 2023).

158. Notably, the Court has issued opinions on the related privileges for the identity of confidential informants and for state secrets. *See* McCray v. Illinois, 386 U.S. 300 (1967); Roviaro v. United States, 353 U.S. 53 (1957); United States v. Reynolds, 345 U.S. 1 (1953). Prior commentators have analyzed the parallel evolution of these privileges and lower courts' analogies between them. *See, e.g.*, Smith, *supra* note 71, at 254–58; Bell, *supra* note 71, at 544–46. In contrast, this Article deliberately shifts focus away from the confidential informant and state secrets doctrines in order to address the privilege for law enforcement methods on its own terms.

159. Shah v. Dep't of Just., 714 F. App'x 657, 659 n.1 (9th Cir. 2017).

district courts in that circuit to follow precedent from other jurisdictions[160] or lump the privilege with related doctrines.[161]

What guidance does exist primarily concerns the second-step balancing procedure. Specifically, the Fifth and D.C. Circuits have adopted a ten-factor balancing test for weighing law enforcement privilege claims[162] drawn from a 1970s civil rights case called *Frankenhauser v. Rizzo*.[163] The factors include (1) the chilling effects of disclosure, (2) whether the information is factual or evaluative, (3) whether it is sought by a criminal defendant, and (4) whether there are alternate sources for the information, *inter alia*.[164] Though not bound, many federal district courts outside the Fifth and D.C. Circuits have also applied the *Frankenhauser* factors.[165] The only other appellate guidance on the balancing procedure is the Seventh Circuit's assertion that balancing is subject to deferential abuse-of-discretion review.[166]

Perhaps because at least some guidance exists regarding the balancing procedure, courts often jump straight to that step without first assessing whether law enforcement has made out the requirements for a threshold claim.[167] This substantially raises the defendant's burden to access information.[168] For instance, to overcome the privilege at the balancing stage, defendants may have to show that information is not merely relevant—the baseline requirement for discovery and subpoenas[169]—but also *necessary* to their defense. This creates a catch-22: It is hard to establish the necessity of information one has not yet seen.

Even if the defense manages to show that information is necessary, law enforcement can undercut that showing by offering an alternate, watered-down, form of proof. For instance, when defendants seek access to information about internet monitoring software and hacking tools, the government

---

160. Pleasant v. Miranda, No. 20-cv-00675, 2021 WL 829735, at *5, *7 & n.3 (C.D. Cal. Jan. 25, 2021) (quoting *In re* Dep't of Investigation, 856 F.2d 481, 484 (2d Cir. 1988)).

161. *See* Hipschman v. Cnty. of San Diego, 738 F. Supp. 3d 1332, 1341 (S.D. Cal. 2024) (citing Kelly v. City of San Jose, 114 F.R.D. 653 (N.D. Cal. 1987)).

162. *In re* U.S. Dep't of Homeland Sec., 459 F.3d 565, 570 (5th Cir. 2006); Tuite v. Henry, 98 F.3d 1411, 1419 (D.C. Cir. 1996).

163. Frankenhauser v. Rizzo, 59 F.R.D. 339, 344 (E.D. Pa. 1973). The Fourth Circuit has mentioned but not expressly endorsed *Frankenhauser*. Cruz v. Bd. of Supervisors, Fairfax Cnty., No. 91-1547, 1993 WL 2667, at *2 (4th Cir. Jan. 27, 1993).

164. *Frankenhauser*, 59 F.R.D. at 344.

165. *See, e.g.*, Wagafe v. Trump, 334 F.R.D. 619, 623–24 (W.D. Wash. 2020); Griffin v. Sigma Alpha Mu Fraternity, No. 09C-04-067, 2011 WL 2120064, at *2 (Del. Super. Ct. Apr. 26, 2011); Al–Kidd v. Gonzales, No. CV 05–093, 2007 WL 4391029, at *5–6 (D. Idaho Dec. 10, 2007); Rhodenizer v. City of Richmond Police Dep't, No. 09CV306, 2009 WL 3334744, at *2 (E.D. Va. Oct. 14, 2009).

166. Dellwood Farms, Inc. v. Cargill, Inc., 128 F.3d 1122, 1125 (7th Cir. 1997).

167. *See, e.g.*, *Griffin*, 2011 WL 2120064, at *2.

168. *See* FED. R. CRIM. P. 17; United States v. Nixon, 418 U.S. 683, 699–700 (1974) (detailing the burden to obtain a criminal subpoena).

169. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 810 (2005).

sometimes responds by offering a law enforcement officer's affidavit asserting information about how the tools work.[170] Courts sometimes view these affidavits as obviating the defendant's need to scrutinize or test the tool directly, despite the clear difficulty of impeaching this testimony without access to the actual software.[171] In theory, that lesser-proof strategy should be unavailable to the government unless it first makes a successful threshold claim to the privilege. If not for privilege, the defense would be entitled to access relevant evidence regardless of what alternate forms of proof may exist.[172] Since the balancing analysis poses such challenges to the defense, threshold claims to the privilege play a significant gatekeeping role. Put simply, if the government is held to have made a threshold claim, it can be game over.

Yet federal appellate courts have done little to explain what constitutes a satisfactory threshold claim to the law enforcement privilege. Some circuits have merely reiterated the broad policy rationale, which Jonathan Manes has termed "the anti-circumvention argument for secrecy."[173] For instance, the initial Second Circuit case to recognize a distinct law enforcement privilege by that name, *In re Department of Investigation*, explained that the privilege's purpose is "to prevent disclosure of law enforcement techniques and procedures,"[174] but provided no further subject-matter requirements for the privilege to attach and no procedural requirements for claimants to assert it.[175] The court did not revisit the privilege until 2010, at which point it held that the privilege applies to "law enforcement techniques and procedures"[176] if disclosure "risks undermining important [police] investigatory procedures,"[177] but offered no additional constraints. The leading First Circuit opinion on the privilege similarly reiterated the rule that it applies to "law enforcement techniques and procedures" if disclosure would "jeopardize future criminal investigations,"[178] but provided no further guidance.

Other federal circuits are likewise sparse on subject-matter requirements, although some have at least fleshed out procedural rules for claiming the privilege. For example, the most recent D.C. Circuit case discussing the privilege,

---

170. *E.g.*, Gov't's Response to Motion to Compel at 13, United States v. Blouin, No. CR16-307 (W.D. Wash. Apr. 25, 2017) (citing Declaration of Detective Robert Erdely ¶ 21 as evidence of how a P2P monitoring software functions).

171. *E.g.*, United States v. Pirosko, No. 12-cr-00327, at 5 (N.D. Ohio Aug. 13, 2013), ECF No. 33.

172. *See* Old Chief v. United States, 519 U.S. 172, 182–83 (1997) (establishing that "evidentiary richness and narrative integrity" can suffice as a theory of relevance for an item of evidence, even if an alternative piece of evidence goes to the same point).

173. Manes, *supra* note 13, at 507.

174. *In re* Dep't of Investigation, 856 F.2d 481, 483–84 (2d Cir. 1988).

175. *Id.*

176. *In re* City of New York, 607 F.3d 923, 944 (2d Cir. 2010) (quoting *In re Dep't of Investigation*, 856 F.2d at 483–83).

177. *Id.* at 936.

178. Puerto Rico v. United States, 490 F.3d 50, 64 (1st Cir. 2007) (quoting *In re Dep't of Investigation*, 856 F.2d at 483–83).

Tuite v. Henry, required that the claim be asserted by the head of a department after "personal consideration by that official."[179] The Tenth Circuit has imposed similar procedural requirements.[180]

The procedural rules that have emerged, however, are plagued by ambiguities, inconsistencies, and open questions. Some courts require the claimant to be a high-level government official,[181] while others permit any law enforcement officer or even a private entity acting on the government's behalf.[182] It is unclear whether the official claiming privilege must review the secret information directly,[183] or simply personally consider the secrecy claim based, for instance, on recommendations from others.[184] Courts are inconsistent at the balancing stage as to whether they are weighing the risk of harm from full public disclosure or from disclosure under a protective order.[185] And while there is general consensus that courts may review the allegedly privileged information in camera, it is unclear whether they *must* do so or whether they are also entitled to pass judgment on the basis of law enforcement affidavits alone.[186]

Only the Fifth Circuit has attempted to specify categories of information to which the law enforcement privilege "probably" does not apply.[187] However, even this attempt offers little clarity. The categories the Fifth Circuit identifies, such as documents from closed investigations, are largely unrelated to law en-

179. Tuite v. Henry, 98 F.3d 1411, 1417 (D.C. Cir. 1996); *see also* Black v. Sheraton Corp. of Am., 564 F.2d 531, 543 (D.C. Cir. 1977); *In re* Sealed Case, 856 F.2d 268, 271 (D.C. Cir. 1988).

180. United States v. Winner, 641 F.2d 825, 831 (10th Cir. 1981).

181. *See, e.g.*, *In re* Sealed Case, 856 F.2d at 271.

182. *Cf.* Kelly v. City of San Jose, 114 F.R.D. 653, 669–70 (N.D. Cal. 1987) (explaining that the claimant must have personal knowledge of the subject material but does not need to be a high-level government official).

183. *See, e.g.*, Moore v. Garnand, No. CV-19-00290-TUC, 2020 WL 1432838, at *3 (D. Ariz. Mar. 24, 2020); *Kelly*, 114 F.R.D. at 669–70.

184. *See Winner*, 641 F.2d at 831–32; United States v. Reynolds, 345 U.S. 1, 8 n.20 (1953).

185. *Compare* Al Otro Lado, Inc. v. Wolf, No. 17-CV-2366-BAS, 2020 WL 3487823, at *3 (S.D. Cal. June 26, 2020) (considering how the risk of harm from full public disclosure could be reduced through use of protective orders), *and Kelly*, 114 F.R.D. at 662 (same), *with* Tuite v. Henry, 98 F.3d 1411, 1417 (D.C. Cir. 1996) (not considering protective orders as one of the factors in protecting the public interest in nondisclosure).

186. *Winner*, 641 F.2d at 832–34; Black v. Sheraton Corp. of Am., 564 F.2d 531, 545 (D.C. Cir. 1977) (recommending in camera review guided by a Vaughn-like index); Friedman v. Bache Halsey Stuart Shields, Inc., 738 F.2d 1336, 1344 (D.C. Cir. 1984).

187. *In re* U.S. Dep't of Homeland Sec., 459 F.3d 565, 571 (5th Cir. 2006) ("Several types of information probably would not be protected, including documents pertaining to: (1) people who have been investigated in the past but are no longer under investigation, (2) people who merely are suspected of a violation without being part of an ongoing criminal investigation, and (3) people who may have violated only civil provisions. Furthermore, the privilege lapses after a reasonable period of time.").

forcement "techniques and procedures," and instead address other public policy issues, such as privacy, that are sometimes lumped under the same privilege banner.[188]

Viewed together, the sole consistent subject-matter requirement for the government to cross the initial threshold of claiming law enforcement privilege is that the privilege applies to law enforcement techniques that must remain secret to be effective. Put another way, federal appellate courts have subtly collapsed the policy rationale for the privilege with the test for assessing threshold claims.

B. *The Problem of Vagueness*

One problem with relying on the policy rationale for law enforcement privilege as the privilege's threshold test is that the policy rationale is vague enough to encompass a broad array of police techniques and procedures that have and should have been successfully litigated in open court.[189] Knowing that police engage in traffic stops, collect cellular location data, or use dogs to sniff drugs could all conceivably help someone evade detection.[190] Taken to its logical extreme, the rationale could cover nearly all law enforcement methods.

To be sure, critics have challenged whether the empirical premises behind the policy rationale hold up at all.[191] Perhaps transparency of methods would deter crimes instead of enabling them, or have little effect.[192] Perhaps secrecy only matters at the margins for highly sophisticated criminal actors.[193] After all, many people commit crimes without adopting countermeasures as obvious as wearing gloves to conceal fingerprints.[194] On the other hand, it is unclear how many *more* people commit crimes wearing gloves than would if fingerprinting were a secret technique. In the absence of empirical evidence that publicity would or would not aid countermeasures, which is exceedingly hard to obtain,[195] plausible arguments exist on both sides of the issue. The uncertainty affords law enforcement a reliable basis from which to argue that disclosure could undermine an extremely broad sweep of investigative methods.

---

188. *See id.*

189. *Cf. Kelly*, 114 F.R.D. at 669.

190. *See, e.g.*, Peter McFarland, Comment to *How Can You Conceal Drugs from Drug-Sniffing Dogs?*, QUORA, https://www.quora.com/How-can-you-conceal-drugs-from-drug-sniffing-dogs [perma.cc/FV77-ZRRL].

191. Manes, *supra* note 13, at 540–42.

192. *Cf.* Jennifer L. Doleac, *The Effects of DNA Databases on Crime*, AMER. ECON. J., Jan. 2017, at 165, 165 (assessing deterrent effects of DNA profiling).

193. Manes, *supra* note 13, at 540–42.

194. *Id.* at 540.

195. Making an empirical assessment more difficult, when courts uphold claims to the privilege, law enforcement assertions about the risks from disclosure necessarily go untested in the real world. Hence, instances of excessive concealment will predictably go undetected. Pozen, *supra* note 68, at 633–34.

As a result, the policy rationale for the privilege is effectively a meaningless constraint. Of course, law enforcement officers do not always claim the privilege. Why? Practically speaking, what limits threshold claims to the law enforcement privilege under current doctrine may be simply the logistical difficulty of deploying a method while keeping it secret. If law enforcement has the technical capacity to keep a method secret while using it in the field, then there is a good chance that current privilege law will let them keep it secret in court as well.

* * *

This Part has described current law enforcement privilege doctrine, observing that federal appellate courts have used the policy rationale for the privilege as the primary subject-matter requirement for asserting a threshold claim. It then argued that the vagueness of the policy rationale gives law enforcement effectively boundless scope to assert privilege claims.

III. A SKEPTICAL ACCOUNT OF EXISTING CRITIQUES

This Part considers existing critiques of the law enforcement privilege. It begins by debunking a generally accepted account of the privilege's history that invites simplistic thinking about the ease of reform. Next, it assesses existing arguments that the privilege should be abolished either entirely or with regard to information possessed by nongovernmental entities. These arguments may well help to mobilize a sympathetic, pro-transparency audience around a shared set of beliefs, but they each have important limitations that make them unlikely to persuade skeptics. The following discussion explains in each instance why the full story is substantially more complex than it may at first appear.

A. *Histories of the Privilege*

Current scholarly consensus holds that no privilege existed for law enforcement investigative methods at common law. Recent articles in the *Duke Law Journal*, the *Berkeley Technology Law Journal*, the *Georgetown Journal of Law and Public Policy*, the *American Criminal Law Review*, and leading legal treatises have all espoused the view that the privilege is ahistorical.[196] Most prominently, Judge Stephen Smith has written a compelling article arguing that former FBI Director J. Edgar Hoover began campaigning for the creation of an evidentiary privilege protecting law enforcement methods in 1956.[197] Judge Smith contends that for two hundred years prior to that time, courts

196. *See, e.g.*, Jonathan David Shaub, *The Executive's Privilege*, 70 DUKE L.J. 1, 20 & n.75 (2020); Manes, *supra* note 13, at 535; Bell, *supra* note 71, at 545–47. *But see* Smith, *supra* note 71, at 233. *See also* 26A WRIGHT, GRAHAM & MURPHY, *supra* note 72, § 5681.

197. Smith, *supra* note 71, at 234 (citing John Edgar Hoover, *The Confidential Nature of FBI Reports*, 8 SYRACUSE L. REV. 2 (1956)).

ruled "on the admissibility of such evidence based on relevance and materiality, without resort to any type of evidentiary privilege."[198] Judge Smith provides strong examples in support. For instance, in one case from 1959, *Williamson v. United States*, the Fifth Circuit considered the location of hidden serial numbers that the FBI used to identify stolen cars.[199] The court held that no prejudice resulted from keeping the location secret, reasoning that there was "nothing to indicate that the location of the serial number would be material" or helpful for impeachment.[200] In other words, consistent with Judge Smith's theory, the Fifth Circuit ruling was based on immateriality, not privilege.[201]

If correct, this history could have direct legal ramifications. The Federal Rules of Evidence grant federal courts authority to develop common-law privileges "in the light of reason and experience."[202] If no privilege for law enforcement methods existed before the mid-twentieth century, then experience might suggest that the privilege could be abolished without harm. The historical record contains some support for this view. Before 1977, no published federal or state court opinion used the phrase "law enforcement privilege," "law enforcement evidentiary privilege," or "law enforcement investigatory privilege."[203] The D.C. Circuit was the first to do so in 1977.[204] The Tenth Circuit followed in 1981,[205] the Second Circuit in 1988,[206] the Fourth and Seventh Circuits in 1997,[207] the Fifth, Ninth, and Federal Circuits in 2006,[208] the First Circuit in 2007,[209] the Sixth Circuit in 2015,[210] and the Eighth Circuit in 2018.[211] Meanwhile, in 1996, in *Jaffee v. Redmond*, the Supreme Court established a careful balancing analysis that federal courts must consider before recognizing

198. *Id.* at 258. Meanwhile, the Ninth Circuit has expressed doubt about whether the privilege exists today. Shah v. Dep't of Just., 714 Fed. App'x 657, 659 & n.1 (9th Cir. 2017).

199. Williamson v. United States, 272 F.2d 495, 496 (5th Cir. 1959).

200. *Id.* at 497.

201. Of course, relevance and materiality determinations may be influenced by the same policy concerns that underly privileges.

202. FED. R. EVID. 501.

203. Search Results: Mentions of Law Enforcement Privilege Prior to 1977, WESTLAW, https://1.next.westlaw.com/Search/Home.html (last visited Feb. 2, 2023) (search "advanced: ('law enforcement privilege' OR 'law enforcement evidentiary privilege' OR 'law enforcement investigatory privilege') & DA (bef 01-01-1977)").

204. Black v. Sheraton Corp. of Am., 564 F.2d 531, 541–42 (D.C. Cir. 1977).

205. United States v. Winner, 641 F.2d 825, 831 (10th Cir. 1981).

206. *In re* Dep't of Investigation, 856 F.2d 481, 483 (2d Cir. 1988).

207. United States v. Hastings, 126 F.3d 310, 311 (4th Cir. 1997); Dellwood Farms, Inc. v. Cargill, Inc., 128 F.3d 1122, 1124 (7th Cir. 1997).

208. *In re* U.S. Dep't of Homeland Sec., 459 F.3d 565, 567 (5th Cir. 2006); Kamakana v. City & Cnty. of Honolulu, 447 F.3d 1172, 1186 (9th Cir. 2006); Marriott Int'l Resorts, L.P. v. United States, 437 F.3d 1302, 1306 (Fed. Cir. 2006).

209. Puerto Rico v. United States, 490 F.3d 50, 61 (1st Cir. 2007).

210. United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. 2015).

211. United States v. Jean, 891 F.3d 712, 715 (8th Cir. 2018).

a new common-law privilege to ensure that the privilege "promotes sufficiently important interests to outweigh the need for probative evidence."[212] None of the federal circuit opinions that initiate the phrase "law enforcement privilege" conducted or even acknowledged the *Jaffee* analysis. One could, therefore, argue that the privilege is invalid in all but the pre-1996 jurisdictions: the D.C., Tenth, and Second Circuits.

Nonetheless, the current scholarly consensus is almost certainly incorrect: It is only the *term* "law enforcement privilege" that is ahistorical. There is nothing new about law enforcement wanting to keep details of investigative techniques secret. And archival sources show that privileges broad enough to encompass those techniques have existed, under various names, for a very long time.

Consider Bishop Atterbury's eighteenth-century treason trial, in which counsel for the Bill of Attainder against Atterbury introduced encrypted letters seized from the mail. A witness claimed to have decrypted the letters and testified that their contents established Atterbury's guilt. The defense sought to challenge the accuracy of the witness's decryption methods.[213] Yet the witness refused to disclose his "method and manner of decyphering" because doing so would "instruct ill-designing men to contrive more difficult cyphers."[214] The testimony was admitted over defense objection on the basis that it was "not consistent with the public safety, to ask the decypherers any questions, which may tend to discover the art or mystery of decyphering."[215] Privileges are public policy-based rules for withholding relevant evidence,[216] so the public safety rationale effectively recognized a privilege for the decryption method.

Of course, the Bishop Atterbury ruling was not binding on United States courts.[217] However, it would be a mistake to assume that the privilege recognized there was *sui generis*. On the contrary, Atterbury's case shows how very

---

212. Jaffee v. Redmond, 518 U.S. 1, 8–12 (1996) (quoting Trammel v. United States, 445 U.S. 40, 51 (1980)).

213. Bishop Atterbury's Trial (1723) 16 How. St. Tr. 323, 496–97 (Gr. Brit.)

214. *Id.* at 497.

215. *Id.*

216. *See* EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE; EVIDENTIARY PRIVILEGES 3 (Richard D. Friedman ed., 2002).

217. The fact that an eighteenth-century English treason trial recognized a privilege to withhold relevant evidence based on a "public safety" rationale does not establish that a similar privilege existed in the United States—or even, for that matter, in England in routine law enforcement cases as opposed to national security or treason cases. *See* 26 WRIGHT, GRAHAM & MURPHY, *supra* note 72, § 5663. *But see* Russell L. Weaver & James T.R. Jones, *The Deliberative Process Privilege*, 54 MO. L. REV. 279, 284 & n.29 (1989). Atterbury's case was especially far from binding precedent because it was a Bill of Attainder proceeding in which the standard rules of evidence did not apply, *see* 16 How. St. Tr. at 560, and the United States Constitution prohibits Bills of Attainder, U.S. CONST. art. I, §§ 9–10. Thank you to Judge Stephen Smith for pointing out these facts.

Notably, Atterbury's defense cited "Coleman's Case" as a precedent in which the government purportedly disclosed a deciphering key, Bishop Atterbury's Trial (1723) 16 How. St. Tr. at 672–73, and permitted the accused to employ defense experts to challenge the deciphering

old the policy concerns are that underly the privilege and how improbable that no United States court would have adopted a similar ruling before the mid-twentieth century. Gaps in the archival record make trial court privilege rulings exceedingly challenging to find, both historically and today, and appellate courts appear to have been silent on this issue for most of United States history. Yet it is far more likely that this silence reflected a general acceptance of at least some form of privilege for law enforcement methods than a universal refutation of the same. The clues from historical treatises, early evidence codes, and what case law is available all support the former conclusion.

Treatises and codes since the late-nineteenth century have described a variety of hazily defined governmental privileges that courts could easily have applied to shield investigative methods, such as a privilege for "the channels through which information of breaches of the law reached the prosecuting authorities."[218] John Henry Wigmore's influential 1905 United States evidence law treatise described "a *privilege of secrecy in general* for *official documents* in an officer's possession . . . and in these precedents no question whatever of international politics or military defence [sic] was involved."[219] Among the precedents Wigmore cited in support of this privilege, which he opined "undoubtedly exists" albeit with uncertain scope,[220] was the Atterbury ruling.[221] And in 1942—more than a decade before Hoover allegedly began campaigning for the creation of a law enforcement privilege[222]—the Model Code of Evidence recognized an "official information" privilege that applied to information if a judge determined that its disclosure "will be harmful to the interests of the government."[223] In short, historical evidence tomes and texts did not need to specify a privilege for law enforcement investigative methods in

---

method, *id.* at 505. This citation appears to have been mistaken. The reference is most likely to Edward Coleman's 1678 treason trial before the King's Bench, in which the prosecution introduced multiple letters as evidence. However, other than translating letters from French to English, there is no indication in the transcript of Coleman's trial that deciphering was ever at issue. *See* Edward Coleman's Trial (1678) 7 How. St. Tr. 1 (KB) (Eng. & Wales).

218. FRANCIS WHARTON, A TREATISE ON THE LAW OF EVIDENCE IN CRIMINAL ISSUES § 513, at 420 (8th ed. 1880). *See also* 1 SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE 342 (Simon Greenleaf Croswell ed., 15th ed. Boston, Little, Brown, & Co. 1892) (describing a privilege for "the channel of communication [to law enforcement], or all that was done under it").

219. 4 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 2375, at 3336 (1st ed. 1905); *see also* DANIEL M'KINNEN, THE PHILOSOPHY OF EVIDENCE 92 (London, S. Brooke 1812) ("[A] case, where a decypherer [sic] had given evidence of the meaning of letters without explaining the grounds of his art, and where the prisoner was convicted and executed.").

220. 4 WIGMORE, *supra* note 219, § 2375, at 3335.

221. *Id.* § 2375, at 3336 & n.3.

222. *See* John Edgar Hoover, *The Confidential Nature of FBI Reports*, 8 SYRACUSE L. REV. 2 (1956).

223. MODEL CODE OF EVID. r. 228 (AM. L. INST. 1942). While the Model Code of Evidence is not synonymous with the common law, it reflected the evidence practice that preceded it. *See, e.g.*, *id.* r. 228 cmt. (AM. L. INST. 1942) ("This Rule . . . represents what some commentators regard as the better decisions in the United States.").

particular because protecting information about such methods was just one stick in a broader bundle of governmental privilege powers.

Early cases developed a similar construction of governmental privilege that could easily have applied to law enforcement investigative methods alongside other sensitive information. For instance, in 1903, a federal court for the Western District of Arkansas upheld a privilege for IRS officers' observations made while discharging official duties.[224] In 1931, the Wisconsin Supreme Court recognized a privilege for "such matters as may form the result" of an arson investigation.[225] And in the 1950 case *United States v. Coplon*, Judge Learned Hand recognized a privilege for concealed FBI wiretap records.[226] He identified the privilege as that for "the names or statements of informers," and described it as "an instance" of the state secrets privilege.[227] Labels aside, the privilege that Judge Hand recognized applied to a domestic law enforcement method, namely wiretaps.[228] To be sure, Judge Hand conceded that "[t]his privilege will often impose a grievous hardship, for it may deprive parties . . . to criminal prosecutions of power to assert their rights or to defend themselves."[229] Yet, such hardship cannot disqualify a privilege from existing because, as Judge Hand concluded, it is "a consequence of any evidentiary privilege."[230]

Even the case about hidden vehicle serial numbers on which Judge Smith relies, *Williamson v. United States*, contains contrary evidence of a privilege.

---

224. *In re* Lamberton, 124 F. 446, 451 (W.D. Ark. 1903).

225. Gilbertson v. State, 236 N.W. 539, 541 (Wisc. 1931).

226. United States v. Coplon, 185 F.2d 629, 638 (2d Cir. 1950). Although this well-known case is frequently misread for the questionable proposition that government privileges should always yield in criminal prosecutions, rigorous scrutiny shows that it actually states the opposite and acknowledges governmental privilege in criminal cases despite the harm.

227. *Id.*

228. *Coplon* ultimately held that the prosecution had waived the privilege in that case by submitting the privileged information to the judge to satisfy its burden of proof on a suppression motion, which, in turn, triggered the defendant's Confrontation Clause right. *Id.* ("It is, however, one thing to allow the privileged person to suppress the evidence, and, *toto coelo*, another thing to allow him to fill a gap in his own evidence by recourse to what he suppresses.").

Readers of *Coplon* may be thrown by Judge Hand's reference to his prior opinion in *United States v. Andolschek*, in which he stated that:

[s]o far as [privileged documents] directly touch the criminal dealings, the prosecution necessarily ends any confidential character the documents may possess . . . . The government must choose; either it must leave the transactions in the obscurity from which a trial will draw them, or it must expose them fully.

142 F.2d 503, 506 (2d Cir. 1944). The documents at issue in *Andolschek* would arguably qualify as *Brady* material today because the criminal prosecution in that case was "founded upon those very dealings to which the [privileged] documents relate, and whose criminality they will, or may, tend to exculpate." *Id.* at 506. The fact that privileges must yield to countervailing constitutional rights such as *Brady* or the Confrontation Clause does not negate their existence or force in other circumstances.

229. *Coplon*, 185 F.2d at 638.

230. *Id.*

Judge Smith is correct that the Fifth Circuit relied on immateriality to shield the numbers' secret location. Yet the trial court transcript from the National Archives tells a different story. The prosecution's objection at the 1959 trial was that "it would be *against public policy* to require the public disclosure of the location of an automobile's confidential serial number, since the purpose of a confidential number is to make it difficult for car thieves to conceal thefts by altering these numbers."[231] Once again, privileges are public policy based rules for excluding evidence, so the prosecution's objection was implicitly a privilege claim.[232] Indeed, California courts have protected the same hidden vehicle serial numbers under the state's statutory "official information privilege" since at least 1976.[233]

As Laura Donohue recognized in the related context of the state secrets privilege (which many have similarly argued was invented in its modern form during the mid-twentieth century[234]), there is a risk of overestimating the recent vintage of privileges due to absences of "historical exposition" coupled with the challenge of researching an area of law where "relevant documents are difficult to obtain . . . [and] often heavily redacted."[235] Inconsistent terminology for the various government privileges,[236] and judges' tendencies to blur findings of privilege with findings of immateriality,[237] muddles the issue of novelty further still.

Despite these challenges, the policy dilemma underlying the law enforcement privilege has clearly plagued the legal system for hundreds of years. Most likely, before the phrase "law enforcement privilege" gained prominence among federal courts, judges simply applied different labels to similar privilege rulings. This by no means suggests that the privilege is justified or that the past must control the future. Nor does it undermine the consequence of a shift in terminology. Changing the label of a privilege can both clarify its policy

231. Brief for the United States in Opposition at 6, Williamson v. United States, 362 U.S. 920 (1960) (No. 698) (emphasis added).

232. While a party's objection at trial does not carry precedential weight, it reflects litigants' presumptions about the existence of privileges and suggests that the trial court may have ruled based on a privilege rationale. Since evidence practice exists primarily in the trial courts, the perspectives of litigants and trial judges are an indication of common practice.

233. People v. Moreno, No. B235421, 2013 WL 97317, at *7 (Cal. Ct. App. Jan. 9, 2013); People v. Marghzar, 239 Cal. Rptr. 130, 132–34 (Cal. Ct. App. 1987); *In re* David W., 133 Cal. Rptr. 342, 346 (Cal. Ct. App. 1976).

234. *See, e.g.*, William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85, 92–101 (2005); 26 WRIGHT, GRAHAM & MURPHY, *supra* note 72, § 5663.

235. Donohue, *supra* note 69, at 82, 84–85; *see also* Christina Koningisor, *The De Facto Reporter's Privilege*, 127 YALE L.J. 1176, 1205–43 (2018).

236. *See* 26 WRIGHT, GRAHAM & MURPHY, *supra* note 72, § 5662.

237. *See, e.g.*, United States v. Hoeffener, 950 F.3d 1037, 1043 (8th Cir. 2020); Bishop Atterbury's Trial (1723) 16 How. St. Tr. 323, 496–97 (Gr. Brit.).

rationale and unmoor it from the procedural safeguards that cabined its predecessors.[238] Yet it would be a mistake to characterize the law enforcement privilege as ahistorical. Doing so is not merely factually unsound; it also invites an underestimation of the privilege's intractability and naïve assumptions about the ease of reform.

B. *Abolition*

That a privilege is longstanding does not mean it should persist. In recent years, scholars have argued for "limiting police power and the space in which it operates;"[239] developed abolitionist approaches to police surveillance technologies[240] and forensic methods;[241] and recommended eliminating public prosecutors' "monopoly" on criminal cases,[242] among other proposals. Perhaps police and prosecutors' privilege to conceal investigative methods should go as well.

Without privilege, the baseline subpoena and discovery rules would entitle defendants to information about law enforcement investigative methods by showing mere relevance,[243] meaning "any tendency" to make a fact more or less likely than it would be without the information.[244] There would be no balancing test requiring defendants to prove the necessity of information they have not yet seen and no consideration of whether alternate information might offer an adequate substitute.

On careful consideration, this possibility is undesirable. Making all investigative methods discoverable on a showing of mere relevance would be a poorly calibrated policy. It could effectively prevent law enforcement from using some lawful, constitutional, and reliable methods. In what is known as a "disclose-or-dismiss" dilemma, prosecutors faced with court orders to disclose investigative techniques must choose between jeopardizing the future efficacy of the technique by complying or dropping criminal charges and withdrawing the case. If the risk of leaks from routine disclosures under a protective order

238. This has arguably happened in the Ninth Circuit, where prior case law coalesced around a well-developed procedure for asserting the "official information privilege," *see* Kelly v. City of San Jose, 114 F.R.D. 653 (N.D. Cal. 1987), but a shift in terminology to the "law enforcement privilege" has left courts without clear guidance, *see* Shah v. Dep't of Just., 714 F. App'x 657, 658–59, 659 n.1 (9th Cir. 2017).

239. Amna A. Akbar, *An Abolitionist Horizon for (Police) Reform*, 108 CALIF. L. REV. 1781, 1838 (2020); *see also* Barry Friedman, *Are Police the Key to Public Safety?: The Case of the Unhoused*, 59 AM. CRIM. L. REV. 1597, 1600 (2022).

240. Vincent M. Southerland, *The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies*, 70 UCLA L. REV. 2 (2023).

241. Maneka Sinha, *Radically Reimagining Forensic Evidence*, 73 ALA. L. REV. 879 (2022).

242. I. Bennett Capers, *Against Prosecutors*, 105 CORNELL L. REV. 1561, 1604 (2020); *see also* Cynthia Godsoe, *The Place of the Prosecutor in Abolitionist Praxis*, 69 UCLA L. REV. 164 (2022).

243. *See* Fed. R. Crim. P. 17(c); Fed. R. Crim. P. 16(a).

244. Fed. R. Evid. 401.

is tolerable, then law enforcement can continue using the technique while repeatedly disclosing it in court. But if that risk is intolerable, as with malware exploits that could be destroyed at scale by a single leak, then recurring disclose-or-dismiss dilemmas could entirely end the technique. While some law enforcement techniques should undoubtedly be banned, the decision should depend on more salient characteristics, such as their dangerousness,[245] brutality,[246] unreliability,[247] or bias,[248] not their susceptibility to leaks.

Another reason not to totally abolish the privilege is that it could perversely result in law enforcement maintaining the same level of secrecy through even more socially harmful means. Prosecutors facing disclose-or-dismiss dilemmas might withdraw more criminal charges, maintaining secrecy by allowing alleged perpetrators of dangerous crimes to return to the community where they could harm future victims. Judges might "bend" the rules of evidence to deny discovery based on irrelevance.[249] And police might rely more on the parallel construction technique of conducting an initial investigation with secret methods followed by a second to re-discover evidence using alternate, public methods, leaving courts, prosecutors, and defendants alike unaware that any secret exists at all.[250] In contrast, keeping the privilege as a lawful avenue for justified secrecy could make parallel construction appear all the more unreasonable and encourage judges to curtail it.[251]

C. *Private-Sector Information*

Some courts and litigants have floated another approach to constraining the law enforcement privilege: categorically barring the privilege for information possessed by private actors that sell surveillance and forensic technologies to police.[252] Private corporations dominate the markets for facial

245. *See* Exec. Order No. 14,074, 3 C.F.R. § 371 (2023).

246. *See* Rochin v. California, 342 U.S. 165, 173 (1952).

247. *See, e.g.*, CLARE GARVIE, GEO. L. CTR. ON PRIV. & TECH., A FORENSIC WITHOUT THE SCIENCE: FACE RECOGNITION IN U.S. CRIMINAL INVESTIGATIONS 13 (2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf [perma.cc/6H5M-62M5].

248. *See, e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540, 663–64 (S.D.N.Y 2013).

249. *Cf.* Edward K. Cheng, G. Alexander Nunn & Julia Simon-Kerr, *Bending the Rules of Evidence*, 118 NW. U. L. REV. 295 (2023).

250. *See* HUM. RTS. WATCH, *supra* note 79.

251. Thank you to Angelo Petrigh for this insight.

252. *See, e.g.*, United States v. Ocasio, No. EP-11-CR-2728, 2013 WL 12442496, at *4 (W.D. Tex. May 28, 2013) (order denying Government's Motion to Quash Subpoenas). *Cf.* Mariano-Florentino Cuéllar & Aziz Z. Huq, *Economics of Surveillance*, 133 HARV. L. REV. 1280, 1329 (2020) (reviewing SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019)) (discussing how state and surveillance economics should not be viewed separately because they are deeply entangled).

recognition software,[253] social media[254] and internet surveillance software,[255] DNA analysis software,[256] phone and other digital device hacking technologies,[257] wireless network forensic tools,[258] and more.[259] Why should these vendors gain the government's secrecy benefits without being bound by its public service mission or democratic controls?[260]

Further, why should law enforcement get to extend its secrecy powers, but not its disclosure duties, to its chosen providers? The result enables law enforcement to evade disclosures through outsourcing. *Brady* and statutory discovery apply solely to members of the prosecution team and those acting on their behalf.[261] Therefore, so long as the prosecution team stays ignorant about how a technology works, they can use that technology without disclosing its functional details.[262] Meanwhile, extending the law enforcement privilege to

253. *See, e.g.*, *Biometric Identification*, DATAWORKS PLUS, https://www.dataworksplus.com/bioid.html#face [perma.cc/29NK-A9DQ]; CLEARVIEW AI, https://www.clearview.ai [perma.cc/C2XA-VHTB]; *see also* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1121–22 (2021).

254. *See, e.g.*, Mary Pat Dwyer, *LAPD Documents Reveal Use of Social Media Monitoring Tools*, BRENNAN CTR. FOR JUST. (Sept. 8, 2021), https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-reveal-use-social-media-monitoring-tools [perma.cc/4YL7-GDY9].

255. *See, e.g.*, Ann Woolner, *Hank Asher's Startup TLO Knows All About You*, BLOOMBERG (Sept. 15, 2011, 6:00 PM), https://www.bloomberg.com/news/articles/2011-09-15/hank-asher-s-startup-tlo-knows-all-about-you#xj4y7vzkg [perma.cc/8GX6-4HJT].

256. *See, e.g.*, Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 675 (2018); Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1976 (2017).

257. *See, e.g.*, Michael Price & Zach Simonetti, *Defending Device Decryption Cases*, CHAMPION, July 2019, at 42, 47 & n.101 (2019); LOGAN KOEPKE, EMMA WEIL, URMILA JANARDAN, TINUOLA DADA & HARLAN YU, UPTURN, MASS EXTRACTION: THE WIDESPREAD POWER OF U.S. LAW ENFORCEMENT TO SEARCH MOBILE PHONES 11 (2020), https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf [perma.cc/L6RU-4PZN].

258. *See, e.g.*, *Markets*, GLADIATOR FORENSICS, https://gladiator-forensics.com/markets [perma.cc/26SM-MPFK]; *see also* FLA. DEP'T OF LAW ENF'T, NOTICE OF INTENDED DECISION TO ENTER INTO A SINGLE SOURCE CONTRACT PUR 7778 (2016); Stephanie Sierra, *Oakland Voting on Possible $6 Million Contract to Bring 'Critical' Software to Police, 911 Center*, ABC7 NEWS (July 24, 2024), https://abc7news.com/post/oakland-voting-possible-6-million-contract-bring-critical-software/15087077 [perma.cc/J7K2-QXDL].

259. *See, e.g.*, Elizabeth Joh & Thomas Joo, *The Harms of Police Surveillance Technology Monopolies*, 99 DENV. L. REV. F. 1 (2022); Joh, *supra* note 35, at 20.

260. The privatization of police functions has given rise to an extensive literature discussing possible pros and cons, from enhanced economic efficiency to distortions from profit incentives. *See, e.g.*, Ingrid V. Eagly & Joanna C. Schwartz, *Lexipol: The Privatization of Police Policymaking*, 96 TEX. L. REV. 891, 897 (2018).

261. For an excellent overview of the reach of *Brady* disclosure obligations, *see* Jonathan Abel, *Cop-"Like" ("👍"): The First Amendment, Criminal Procedure, and the Regulation of Police Social Media Speech*, 74 STAN. L. REV. 1199, 1236 (2022).

262. *Cf.* Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1337, 1376 (2021).

private vendors blocks defendants' alternate avenue for discovery through third-party subpoenas.

Case law on whether the privilege expires at the edge of government is mixed. At least one federal district court considering a defense request for source code for an internet surveillance software held that the privilege "applies only to *government* documents."[263] The prosecution's apparent double dipping vexed the court: The prosecution initially denied discovery by claiming ignorance of how the software worked[264] and maintaining that the software was controlled by a private vendor,[265] but then later asserted privilege to stop the defense from subpoenaing the vendor.[266] A different federal district court, however, upheld the privilege for an executable copy of the same software.[267] It reasoned that the privilege applied because the software, while owned by a private company, "is exclusively used by law enforcement officers."[268] In yet a third case, prosecutors argued that the privilege should extend to "a quasi-law enforcement agency" and that private developers of surveillance and forensic software can qualify.[269] Meanwhile, nothing in current appellate doctrine stops the privilege from shielding information possessed by private entities, even information that no one in the government has ever seen.

While superficially appealing, a public/private constraint on the privilege is ultimately unpersuasive. The security value of a secret does not depend on whether the government or a private entity possesses it. A leak can destroy a malware exploit regardless of whether law enforcement purchased it or developed it in house. Related doctrines recognize this reality and extend government secrecy powers to shield private-sector information. Information in an investigative file can be privileged even if it came from a private informant.[270] The state secrets privilege extends to military and diplomatic secrets possessed

263. United States v. Ocasio, No. EP-11-CR-2728, 2013 WL 12442496, at *1–2 (W.D. Tex. May 28, 2013) (order denying Government's Motion to Quash Subpoenas).

264. *Id.* at *3.

265. *Id.*

266. *Id.* at *4.

267. United States v. Pirosko, No. 12-cr-00327, at 1–2 (N.D. Ohio, Aug. 13, 2013) (order denying motion to compel discovery and request to extend pretrial motion deadline).

268. *Id*.

269. United States' Response to Defendant's Motion to Compel Prod. (Doc. 19) at 12, United States v. Dang, No. 16-10027-01 (D. Kan. Sept. 26, 2016), ECF No. 23.

270. *See, e.g.*, Capitol Vending Co. v. Baker, 35 F.R.D. 510, 510–11 (D.D.C. 1964) (privilege for "documents that the government is using in connection with an investigation of possible violations of criminal laws" without limitation as to the origins of the documents); Gilbertson v. State, 236 N.W. 539, 540 (Wis. 1931) (privilege for reports and notes of investigations, including "testimony of all persons taken in investigations conducted by the state fire marshal or his deputies"); *see also* Note, *Discovery of Government Documents and the Official Information Privilege*, 76 COLUM. L. REV. 142, 158–59 (1976) (discussing courts' reluctance to order disclosure of law enforcement files while investigations are ongoing).

by private contractors.[271] Most federal circuits have held that the FOIA exemption for inter-agency and intra-agency memoranda shields information possessed by private consultants who are working for the government.[272] The Invention Secrecy Act permits the United States Patent and Trademark Office to bar disclosures of private sector inventions that might be "detrimental to the national security."[273] And under the Atomic Energy Act, information is famously "born secret"[274]; the Act automatically classifies nuclear discoveries at inception, even if made by private entities with no government aid or involvement.[275] Relatedly, privatization scholars considering whether other (non-secrecy) governmental immunities and constraints should extend to private contractors have repeatedly argued that the dividing line should track the nature of the activity, not the nature of the actor.[276]

What about information that no one in the government has ever seen? Should the privilege extend there too? If law enforcement officials had to personally review information before claiming privilege, perhaps they would be less likely to double dip by asserting privilege over private-sector information while simultaneously claiming ignorance about it for purposes of *Brady* and statutory discovery. This issue is ripe for litigation. The D.C. Circuit has held that the law enforcement privilege must be claimed by a governmental official who has personally "seen and considered *the contents of the documents*."[277] Other circuits seemingly lack this requirement.[278] Ultimately, however, while a universal personal review requirement would help to ensure that everybody claiming the government's privilege is democratically accountable, it is unlikely to entirely stop double-dipping; law enforcement officials beyond the prosecution team could still assert the privilege while leaving the prosecution in the dark and free from *Brady* or statutory discovery obligations. In other

271. *See, e.g.*, Crater Corp. v. Lucent Techs., Inc., 423 F.3d 1260, 1265–66 (Fed. Cir. 2005).

272. *See* Rojas v. Fed. Aviation Admin., 989 F.3d 666 (9th Cir. 2021) (en banc).

273. 35 U.S.C. § 181.

274. Peter Galison, *Removing Knowledge*, 31 CRITICAL INQUIRY 229, 232 (2004).

275. *See* Laura K. Donohue, *Functional Secrecy*, *in* JUDGING NATIONAL SECURITY: THE EVOLVING JUDICIAL ROLE IN NATIONAL SECURITY CASES (Robert M. Chesney & Steven I. Vladeck, eds., forthcoming 2021) (manuscript at 13), http://dx.doi.org/10.2139/ssrn.3450806.

276. *See, e.g.*, Kate Sablosky Elengold & Jonathan D. Glater, *The Sovereign in Commerce*, 73 STAN. L. REV. 1101, 1108 (2021); Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1371 (2003).

277. Friedman v. Bache Halsey Stuart Shields, Inc., 738 F.2d 1336, 1342 (D.C. Cir. 1984) (emphasis added) (quoting Kerr v. U.S. Dist. Ct. for N. Dist. of Cal., 511 F.2d 192, 198 (9th Cir. 1975)).

278. *See, e.g.*, *In re* City of New York, 607 F.3d 923, 944 (2d Cir. 2010) (describing privilege claimant's burden of proof without specifying a requirement for claimants to have a government official personally review the documents' contents); United States v. Amodeo, 44 F.3d 141, 142, 145 (2d Cir. 1995) (remanding a case involving a non-governmental third party—albeit an appointed Court Officer investigating pursuant to a Consent Decree—asserting the privilege to block disclosure of documents, thereby implicitly accepting the premise that non-governmental actors can claim the privilege, rather than a government official).

words, even if courts were to strictly limit the privilege to information possessed by some part of the government, not by private entities, it would not solve the double-dipping problem.

* * *

This Part has examined the strengths and infirmities of the plausible arguments against law enforcement privilege. It initially drew on archival research to debunk the current scholarly consensus that the privilege is an ahistorical, mid-twentieth-century invention. It then explained why completely abolishing the privilege could be harmful to both public safety and law enforcement transparency and accountability. Finally, it considered and critiqued arguments that the privilege should not apply to information possessed by private entities. The following Part offers an alternative to reasonably constrain law enforcement privilege claims while minimizing risk to law enforcement efficacy.

IV. LIMITING THRESHOLD CLAIMS

We are now back to the conundrum with which we started. Criminal defendants sometimes have legitimate interests in accessing information about law enforcement methods, and police and prosecutors sometimes have legitimate interests in withholding that information. Yet, empowering the state to keep this information secret creates the risk that the secrecy power will be abused. Meanwhile, judges deciding whether to uphold a privilege claim must resolve an issue of specialized expertise without the benefits of a full adversarial process to educate them about the law and facts. The result leaves courts in a bind and disadvantages the entire truth-seeking process in cases that implicate life, liberty, and police accountability.

The current doctrine's vagueness makes this conundrum worse. Federal appellate case law simply reiterates the privilege's policy rationale as the test for asserting threshold claims and, consequently, imposes virtually no meaningful constraint on law enforcement's secrecy power. The policy rationale supposedly motivating the privilege—that disclosure of investigative methods would risk countermeasures—could theoretically apply to almost any investigative technique. Vagueness invites law enforcement to overclaim the privilege, whether to conceal mistakes and negligence, to hide unlawful and unconstitutional conduct, or simply to avoid the hassle and inconvenience of having investigative methods challenged in court. As one federal judge opined, "[i]n a society where government is supposed to be open, where it is supposed to be the servant of and responsive to the people . . . does it make sense for courts to create a body of privilege doctrine that sweeps so broadly[?]"[279]

For the criminally accused, the consequences could not be more serious or more urgent. A federal defendant in New York was sentenced to a decade

279. Kelly v. City of San Jose, 114 F.R.D. 653, 659 (N.D. Cal. 1987).

in prison after being denied access to software that the defendant claimed had "provided the 'bulk of the evidence' for his conviction."[280] A federal defendant in Wisconsin was sentenced to five years in prison after being denied access to investigative software that provided the sole evidence of certain criminal charges in his case.[281] A federal defendant in Missouri faced life in prison after being denied access to source code, manuals, and an executable copy of a "law enforcement software program" used to establish probable cause.[282] A federal defendant in Ohio was sentenced to twenty years in prison after being denied access to similar software used to establish probable cause.[283] In each of these cases, and many more like them, the law enforcement privilege barred defendants from fully scrutinizing the evidence against them.

The problem is poised to grow as more law enforcement agencies deploy AI and other software-driven investigative methods in the field while keeping secret the training data, code, models, and functions that control the technology. Federal law enforcement has been conducting "online surveillance and sting operations"[284] and developing "custom malware" to deanonymize users, hack into servers,[285] and investigate the darknet[286] for years. At the same time, federal prosecutors have been arguing that the law enforcement privilege should protect these methods.[287] But law enforcement hacking will not remain a federal enterprise, nor will privilege claims for such methods stay cabined in the comparatively small percentage of federal criminal cases nationwide.[288] Commercial spyware is a rapidly growing, twelve billion dollar industry eager for new law enforcement customers.[289] Over the past ten years, law enforcement's use of secretive commercial hacking tools has spread from highly specialized federal agencies to state, local, tribal, and territorial authorities, where

280. United States v. Clarke, 979 F.3d 82, 97 (2d Cir. 2020).

281. United States v. Owens, 18 F.4th 928 (7th Cir. 2021).

282. United States v. Hoeffener, 950 F.3d 1037 (8th Cir. 2020).

283. United States v. Pirosko, 787 F.3d 358 (6th Cir. 2015).

284. KRISTIN FINKLEA, CONG. RSCH. SERV., IF12172, THE DARK WEB: AN OVERVIEW (2022).

285. KRISTIN FINKLEA, CONG. RSCH. SERV., R44101, DARK WEB 7, 13 (2017).

286. FINKLEA, *supra* note 284.

287. *See, e.g.*, *Pirosko*, 787 F.3d at 364.

288. *See* Jennifer Lawinski, *Cybercrime Forces Local Law Enforcement to Shift Focus*, DARK READING (Feb. 26, 2025), https://www.darkreading.com/cyberattacks-data-breaches/cybercrime-forces-local-law-enforcement-to-shift-focus [perma.cc/52V6-2KUD].

289. *See* Asaf Lubin, *Selling Surveillance*, 85 OHIO ST. L.J. (forthcoming 2025) (manuscript at 3) (citing Mark Mazzetti, Ronen Bergman & Matina Stevis-Gridneff, *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Jan. 28, 2023), https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html [perma.cc/3AZ3-8B7F]) http://dx.doi.org/10.2139/ssrn.4323985.

the risk of abuse may be higher and harder to remedy.[290] As more and increasingly diverse law enforcement agencies adopt these types of tools, privilege claims will follow. The time to fix the privilege is now.

This Part proposes an easily administrable way for courts to conduct more meaningful judicial review of law enforcement secrecy claims: assess threshold claims by reference to law enforcement's own pre-dispute conduct. Courts should demand to know the conditions that law enforcement previously imposed on access to the allegedly privileged information. Were recipients required to sign a nondisclosure agreement? If so, what were the terms? Was access revoked or information returned at the close of each investigation? Where and how was the information stored? Was access supervised, logged, or required to occur at a secure, monitored location? The answers to these questions reveal law enforcement's own tolerance for leaks and should thus establish a transparency floor: At a minimum, if the court can impose protective-order safeguards that match or exceed what law enforcement previously required, then disclosure does not significantly increase the risk of the secret getting out. In those circumstances, judges should have no qualms about denying the privilege and ordering disclosure.

Factoring law enforcement's pre-dispute conduct into courts' assessment of privilege claims will cabin law enforcement's secrecy power while minimizing risks to law enforcement efficacy. Appellate courts should use their common-law authority over evidentiary privileges to require that claimants divulge the conditions of prior dissemination when asserting a threshold claim to the law enforcement privilege. Meanwhile, trial courts should include these requirements in their standing orders for how to assert a privilege claim. If courts fail to do so, or in states where courts lack common-law authority over privileges,[291] legislators should codify the requirements, either in evidence codes or in Community Control Over Police Surveillance laws.[292] This Part concludes by addressing likely counterarguments and explaining why they are ultimately unpersuasive.

A. *Pre-Dispute Conduct as Circumstantial Evidence*

To explain the benefits of using law enforcement's prior conduct as a default floor for transparency in the courts, it will help first to sharpen the policy

290. *Compare* Libor Jany, *Pasadena Police Banking on Phone-Hacking Tool to Solve Cold Case Murder*, L.A. TIMES (Mar. 3, 2023, 5:00 AM), https://www.latimes.com/california/story/2023-03-03/pasadena-police-banking-on-phone-hacking-tool-to-solve-cold-case-murder [perma.cc/HCP2-P6U9], *and* Lorenzo Franceschi-Bicchierai, *This is the 'GrayKey 2.0,' the Tool Cops Use to Hack Phones*, MOTHERBOARD (Sept. 30, 2022, 11:01 AM), https://www.vice.com/en/article/this-is-the-graykey-20-the-tool-cops-use-to-hack-phones [perma.cc/M9JC-G4TJ], *with* Adrianne Jeffries, *Meet Hacking Team, the Company that Helps the Police Hack You*, THE VERGE (Sept. 13, 2013, 10:30 AM), https://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers [perma.cc/2QQW-ZA39].

291. *See* CAL. EVID. CODE. § 911 (West 2009).

292. *See* Southerland, *supra* note 240.

justification for the law enforcement privilege. Existing appellate opinions state the rationale far too abstractly: "to prevent disclosure of law enforcement techniques and procedures";[293] to avoid "undermining important [police] investigatory procedures";[294] to bar disclosures that might "jeopardize future criminal investigations";[295] and to conceal "investigative techniques or sources."[296] Properly unpacked, the logic behind these nebulous assertions is not merely that secrecy helps to prevent countermeasures, because *information disclosed in court, subject to a protective order, is still secret information*. The privilege can thus be justified only when disclosure under a protective order poses an untenable risk of leaks.[297] Although current doctrine never states this, the logic underlying the privilege is not simply curtailing the risk of countermeasures but, more precisely, curtailing the risk of leaks.

The problem remains of how courts should assess the risk of leaks, including both their probability and their magnitude of harm. Protective orders, after all, are not foolproof. They can minimize risk by restricting disclosures to attorneys or pre-vetted experts whom both parties agree are trustworthy.[298] They can require the recipient, on pain of civil[299] and criminal contempt, to use the information solely for a particular case and to return or destroy it after the proceeding ends.[300] They can require that documents be reviewed under supervision at a particular secure location, such as a SCIF (sensitive compartmented information facility).[301] They can require that the recipients obtain a

293. *In re* Dep't of Investigation, 856 F.2d 481, 484 (2d Cir. 1988).

294. *In re* City of New York, 607 F.3d 923, 936 (2d Cir. 2010).

295. Puerto Rico v. United States, 490 F.3d 50, 64 (1st Cir. 2007).

296. Tuite v. Henry, 98 F.3d 1411, 1413 (D.C. Cir. 1996).

297. As a result, any protection the law enforcement privilege affords from liability is unavoidable collateral. That distinguishes the privilege from most communications privileges, which incentivize uninhibited communications by offering a shield from both leaks and liability. *See* Upjohn Co. v. U.S., 449 U.S. 383, 389 (1981) (discussing the rationale of attorney client privilege). Hence, past crimes, fraud, and negligence disclosed to one's attorney cannot be revealed to the opposing party, even under a foolproof protective order. *In re* Grand Jury Subpoenas, 144 F.3d 653 (10th Cir. 1998).

298. *See, e.g.*, N.Y. CRIM. PROC. LAW § 245.70 (McKinney 2024).

299. *E.g.*, 18 U.S.C. § 401 (2016).

300. Elizabeth Miles, *Protective Orders: Does Yours Cover All the Bases?*, NAT'L L. REV. (Sept. 24, 2019) https://natlawreview.com/article/protective-orders-does-yours-cover-all-bases [perma.cc/4GXL-MSVG].

301. CRIM. PROC. § 245.70.

security clearance.[302] Still, protective orders sometimes fail. Attorneys or experts may leak information despite the threat of sanction,[303] and leaks can be difficult to trace and remedy.[304]

The answer to this problem is simple: Courts should use law enforcement's pre-dispute conduct regarding the confidentiality of the information as circumstantial evidence of an acceptable risk of leaks. Courts should demand to know how law enforcement previously treated the allegedly privileged information. As an initial matter, if law enforcement failed to take reasonable care before coming to court, then in most cases judges should be able to avoid the difficult task of digging further and simply default to ordering disclosure. Second, even if the government manages to cross the initial threshold by showing reasonable care, it should often still be possible for courts to accommodate defense access. Here is a simple procedure to do so. Courts should compare how law enforcement itself previously treated the information to the safeguards that a protective order could afford. If judges can craft a protective order that matches or exceeds the protections that law enforcement previously imposed, then ordering disclosure would not create a significant new risk of leaks and courts should, once again, default to ordering disclosure.

This approach would have multiple advantages. Substantively, law enforcement's pre-dispute conduct poses less risk of insincerity than post-dispute testimony because it requires more foresight and deliberation to falsify.[305] While both post-dispute courtroom testimony and pre-dispute conduct can be falsified, the motive to falsify is likely to increase once litigation begins. Institutionally, relying on the pre-dispute conduct would leverage law enforcement's security expertise to assist judicial review, transforming a comparative weakness of the courts into a boon. Procedurally, evidence about the conduct could be adjudicated publicly in fully adversarial hearings without revealing the allegedly privileged information. Parties could create more robust records for appeal. Courts could develop common-law reasoning about how best to

302. Bell, *supra* note 71, at 551. *See also* Response in Opposition to the Government's Renewed Motion for Protective Order Pursuant to Section 3 of the Classified Information Procedures Act at 5, United States v. Trump, 700 F. Supp. 3d 1126 (S.D. Fla. 2023) (No. 23-80101-CR), ECF 104 (discussing "documents [that] can only be viewed after full security clearance is secured" by defense counsel).

303. *In re* City of New York, 607 F.3d 923, 935 n.12 (2nd Cir. 2010).

304. *Id.* at 936.

305. *Cf.* United States v. Zenni, 492 F. Supp. 464 (E.D. Ky. 1980) (quoting 4 JACK B. WEINSTEIN, MARGARET A. BERGER & JOSEPH M. MCLAUGHLIN, WEINSTEIN'S EVIDENCE ¶ 801(a)[1] (Joseph Fogel ed., 1996)) (explaining why nonassertive verbal conduct is not subject to the hearsay rule because "when a person acts in a way consistent with a belief but without intending by his act to communicate that belief," the person's sincerity is not at question); FED. R. EVID. 801 (excluding non-assertive statements from the hearsay rule).

evaluate this type of evidence. Legislative, regulatory, and civilian oversight commissions could learn more about police practices.[306]

Normatively, this approach would discourage courts from presuming defense counsel and their experts are untrustworthy while giving police and prosecutors the benefit of the doubt. To be sure, defense attorneys have leaked information in some cases.[307] But so have law enforcement officers.[308] Fortunately, these known incidents are few and far between.[309] And while defense counsel's duty of zealous advocacy might indicate a higher risk compared to law enforcement's more generalized duties to the public,[310] other facts suggest the risks may be equivalent: Both law enforcement and defense counsel can be subject to disciplinary sanction, both operate within a range of institutional structures and oversight mechanisms, and many defense counsel, like law enforcement, are public employees. Alternately, it could be even riskier to disclose to law enforcement insiders, for whom punishment may be limited to loss of employment and civil liability for breach of contract, than to defense counsel outsiders under a protective order that can be enforced through threat of criminal contempt. Without empirical evidence establishing that defense counsel and their experts are less trustworthy than law enforcement and their contractors, there is no good reason for courts to categorically favor one over the other without consideration of individual factors on a case-by-case basis.

Given the advantages, this proposal for how courts should assess law enforcement privilege claims might seem obvious. But current doctrine fails to require law enforcement to disclose information about prior dissemination.[311]

---

306. *See generally* Sharon R. Fairley, *Survey Says?: U.S. Cities Double Down on Civilian Oversight of Police Despite Challenges and Controversy*, 2020 CARDOZO L. REV. DE NOVO 1.

307. *See, e.g.*, United States v. Stewart, 590 F.3d 93, 109–10 (2d Cir. 2009); Bob Egelko, *Lawyer Admits Leaking Balco Testimony / He Agrees to Plead Guilty—Prosecutors Say They'll End Effort to Jail Reporters*, SFGATE (Feb. 14, 2007), https://www.sfgate.com/bayarea/article/LAWYER-ADMITS-LEAKING-BALCO-TESTIMONY-He-agrees-2617522.php [perma.cc/UX2K-B88J].

308. *See, e.g.*, Spencer S. Hsu, Peter Hermann & Tom Jackman, *D.C. Police Officer Arrested, Accused of Leaking Info to Proud Boys Leader*, WASH. POST (May 19, 2023, 2:09 PM), https://www.washingtonpost.com/dc-md-va/2023/05/19/dc-police-officer-arrested-obstruction-jan6 [perma.cc/6NU3-QGPJ]; Dhruv Mehrota, *A Police App Exposed Secret Details About Raids and Suspects*, WIRED (Jan. 11, 2023, 9:12 AM), https://www.wired.com/story/sweepwizard-police-raids-data-exposure [perma.cc/S68K-CVNK].

309. If defense counsel regularly breached protective orders, one would expect prosecutors to produce evidence of that fact whenever they argue against disclosure. They do not.

310. *Compare* Eric S. Fish, *Against Adversary Prosecution*, 103 IOWA L. REV. 1419, 1467 (2018), *with* Charles J. Ogletree, Jr., *Beyond Justifications: Seeking Motivations to Sustain Public Defenders*, 106 HARV. L. REV. 1239, 1246–47 (1993).

311. *See, e.g.*, United States v. Jean, 891 F.3d 712 (8th Cir. 2018) (deciding a child pornography case without addressing efforts of either law enforcement or the developers of the website to maintain confidentiality).

It also fails to discount the magnitude of harm a leak would cause by the probability it will occur under a protective-order disclosure.[312] The leading appellate opinions never mention pre-dispute confidentiality.[313] None of the *Frankenhauser* balancing factors include confidentiality.[314] While some federal district courts have considered confidentiality when assessing law enforcement privilege claims,[315] many have not.[316] Similarly, some district courts have considered the safeguards a protective order could provide.[317] Others have not.[318] At least one attempted to discount the secrecy interest according to protective-order conditions and was overruled on appeal.[319]

Although law enforcement privilege doctrine has thus far failed to focus on pre-dispute confidentiality, doing so would be far from unprecedented. One cannot generally share information willy-nilly and then turn around and claim that it is privileged in court. On the contrary, a pre-dispute "reasonable expectation of confidentiality" is an essential element of many nongovernmental privileges, such as the attorney-client, spousal, clergy-penitent, and psychotherapist-patient privileges.[320] Scholars have theorized certain aspects of this requirement. Prominently, Wigmore characterized it as an incentive for

312. Instead, the Tenth Circuit assertion that the privilege is "based primarily on the harm to law enforcement efforts which might arise from public disclosure," United States v. Winner, 641 F.2d 825, 831 (10th Cir. 1981) (quoting Black v. Sheraton Corp., 564 F.2d 531, 541 (D.C. Cir. 1977)), the Second Circuit assertion that the privilege applies if disclosure "risks undermining important [police] investigatory procedures," *In re* City of New York, 607 F.3d 923, 936, 944 (2d Cir. 2010), and the First Circuit contention that the privilege applies if disclosure would "jeopardize future criminal investigations," Puerto Rico v. United States, 490 F.3d 50, 64 (1st Cir. 2007), invite courts to presume a leak and assess solely its magnitude of harm. *Cf.* Peter Z. Grossman, Reed W. Cearley & Daniel H. Cole, *Uncertainty, Insurance and the Learned Hand Formula*, 5 LAW, PROBABILITY & RISK 1 (2006).

313. *See supra* Section II.A.

314. *Id.*

315. For an exemplary confidentiality analysis, see *Torres v. Kuzniasz*, 936 F. Supp. 1201, 1210 (D.N.J. 1996).

316. *See, e.g.*, *Puerto Rico*, 490 F.3d at 65, 67, 69–70 (mentioning the FBI's interest in maintaining or preserving allegedly confidential law enforcement techniques without any analysis of steps that the FBI did or did not take to ensure confidentiality up to that point). When courts do engage in a confidentiality analysis, it is often superficial. *See, e.g.*, United States v. Rigmaiden, 844 F. Supp. 2d 982, 994–95 (D. Ariz. 2012).

317. *See, e.g.*, United States v. Pierce, No. 20-cr-40068, 2021 WL 1949355, at *3–4 (D. Kan. May 14, 2021) (order granting motion to compel); Preston v. Malcolm, No. 09–3714, 2009 WL 4796797, at *7 (D.N.J. Dec. 8, 2009); Kelly v. City of San Jose, 114 F.R.D. 653, 666 (N.D. Cal. 1987).

318. *See, e.g.*, United States v. Hoeffener, No. 16CR00374, 2017 WL 3676141, at *18–19 (E.D. Mo. Aug. 25, 2017) (order denying motion to compel).

319. *In re* City of New York, 607 F.3d 923, 935–37 (2d. Cir. 2010).

320. Edward J. Imwinkelried, *The Dangerous Trend Blurring the Distinction Between a Reasonable Expectation of Confidentiality in Privilege Law and a Reasonable Expectation of Privacy in Fourth Amendment Jurisprudence*, 57 LOY. L. REV. 1, 3 (2011).

people in privileged relationships to communicate.[321] More recently, scholars have questioned whether it valuably limits the scope of privilege protections[322] or conflicts with peoples' actual perceptions about their communications (and should thus be abolished).[323] Still other scholars have untangled its relationship to the reasonable expectations of privacy test in Fourth Amendment jurisprudence.[324]

There is another explanation: The confidentiality requirement is an information-forcing function; it serves as a signal for the value of secrecy that can be adjudicated publicly in a fully adversarial hearing without exposing the allegedly privileged information.[325]

Similarly, trade secret claimants must show that, pre-dispute, they undertook reasonable efforts to maintain the secrecy of their alleged intellectual property.[326] For instance, the Ninth Circuit invalidated a trade secret because a company failed to take reasonable secrecy precautions when it permitted employees to remove information from the premises and to retain possession after their employment ended.[327] (Compare that ruling to *Budziak*, in which no court considered the FBI's similar conduct when assessing its claim to the law enforcement privilege.[328]) Scholars have debated various justifications for this "reasonable efforts" component of trade secret law.[329] The theory most

---

321. *See, e.g.*, Edward J. Imwinkelried, *The New Wigmore: An Essay on Rethinking the Foundation of Evidentiary Privileges*, 83 B.U. L. REV. 315, 319–20 (2003).

322. *E.g.*, Melanie B. Leslie, *The Costs of Confidentiality and the Purpose of Privilege*, 2000 WIS. L. REV. 31 (2001).

323. *E.g.*, Paul R. Rice, *A Bad Idea Dying Hard: A Reply to Professor Leslie's Defense of the Indefensible*, 2001 WIS. L. REV. 187 (2001); Paul R. Rice, *Attorney-Client Privilege: The Eroding Concept of Confidentiality Should be Abolished*, 47 DUKE L.J. 853 (1998).

324. *E.g.*, Imwinkelreid, *supra* note 320; Robert P. Mosteller & Kenneth S. Broun, *The Danger to Confidential Communications in the Mismatch Between the Fourth Amendment's "Reasonable Expectation of Privacy" and the Confidentiality of Evidentiary Privileges*, 32 CAMPBELL L. REV. 147 (2010); *see also* Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485 (2018).

325. Whether communicants spoke in a room with others present, closed a door or window, used encrypted email, or otherwise undertook reasonable efforts to block eavesdroppers, can often be determined without revealing the contents of the communications themselves. *E.g.*, United States v. Gann, 732 F.2d 714, 722–23 (9th Cir. 1984).

326. Trade secret claims brought under the federal Defend Trade Secrets Act and the Uniform Trade Secret Act must establish that trade secret holders undertook reasonable efforts to maintain the secrecy of their alleged trade secrets. Defend Trade Secrets Act, 18 U.S.C. § 1839(3); UNIF. TRADE SECRETS ACT, § 1(4) (amended 1985), 14 U.L.A. 437 (1990).

327. *See* Buffets, Inc., v. Klinke, 73 F.3d 965, 969–70 (9th Cir. 1996).

328. *See supra* notes 142–148 and accompanying text.

329. Theories range from characterizing the requirement as a vestige of common-law property rights, to a notice mechanism to avoid unintentional misappropriation, to a means of balancing the costs and benefits of protecting intellectual property versus disseminating knowledge. *See* Robert G. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions*, *in* THE LAW AND THEORY OF TRADE SECRETS: A HANDBOOK OF CONTEMPORARY RESEARCH 46, 52 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1153 & n.148 (2000);

pertinent here is that it generates circumstantial evidence showing the fact and value of secrecy.[330]

Prior scholars of government secrecy have likewise emphasized characteristics of secrets other than their contents. To name just a few, in a well-developed analysis of the distinction between deep and shallow secrecy, David Pozen observes that "how many people know of [the secret], what sorts of people know, how much they know, and [when] they know" can help to "describe, assess, and compare secrets, without having to judge what they conceal."[331] Heidi Kitrosser advocates for the public to know about the "existence and basic nature" of political branch secrets as well as the "policy of secrecy" governing them.[332] And Mary Cheh argues that courts should concentrate on "policies or processes of concealment" rather than try "to review the validity of particular secrecy decisions."[333] Each of these approaches shares the same key kernel of wisdom that secrets can be judged by their metadata rather than by their innards.

In sum, if courts tied law enforcement privilege claims to pre-dispute confidentiality, they would be in good company.

B. *Application*

How would this work in practice? Recall *Budziak* in which the FBI lost the source code for an internet surveillance software system and failed to track other copies of the code in the hands of a private contractor and its departing personnel.[334] That lax security should have undercut a claim to privilege because the court could have easily exceeded the FBI's own prior safeguards by requiring the defense to return or destroy the code after examining it. In the actual case, the court eventually imposed even higher protections. After the Ninth Circuit overruled the privilege, the district court ordered disclosure to "occur in a space and on a computer designated by the FBI" with an FBI agent

---

Peter S. Menell, *Economic Analysis of Network Effects and Intellectual Property*, 34 BERKELEY TECH. L.J. 219, 244 (2019). *See also* David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, J. ECON. PERSPS., Winter 1991, at 61, 69.

330. *See, e.g.*, Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. 2409, 2446 & n.217 (2019); *see also* Bone, *supra* note 329, at 47.

331. David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 257, 267 (2010).

332. Heidi Kitrosser, *Secrecy and Separated Powers: Executive Privilege Revisited*, 92 IOWA L. REV. 489, 514–15 (2007).

333. Mary M. Cheh, *Judicial Supervision of Executive Secrecy: Rethinking Freedom of Expression for Government Employees and the Public Right of Access to Government Information*, 69 CORNELL L. REV. 690, 730 (1984).

334. *See supra* notes 149–153 and accompanying text.

"present for the review."[335] Had the district court assessed pre-dispute confidentiality when initially ruling on the threshold privilege claim, it might have denied the privilege in the first place and avoided overruling on appeal.

Or consider *Pirosko*, in which the district court and Sixth Circuit both upheld the privilege for another internet surveillance software program, reasoning that defense access risked enabling criminal actors to "find ways to avoid these surveillance systems"[336] and "frustrate future surveillance efforts."[337] As it turns out, the software developer's own website boasts that "[m]ore than 10,000 law enforcement officers in all 50 U.S. states and in 102 countries around the globe [h]ave been trained on our technology."[338] Those ten thousand people have access under what can be no more than contractual promises of confidentiality. A protective order could easily exceed that safeguard and be enforceable not merely through contractual liability, but also through civil and criminal contempt and professional discipline.[339] A comparison between prior dissemination to the safeguards available for in-court disclosures should have led the court to accommodate defense access.

A similar analysis would apply to other surveillance and forensic technologies that are widely distributed under mere contractual nondisclosure orders. For an easy example, Grayshift, a company that sells hacking services to law enforcement to "extract evidence from mobile devices,"[340] explicitly warns its contracting partners that information is subject to court-ordered disclosure. Its contracts with police departments state that "disclosure of Confidential Information that is legally compelled to be disclosed pursuant to a subpoena, summons, order or other judicial or governmental process shall not be considered a breach of this Agreement."[341] There is no reason, then, for Grayshift users to expect secrecy from the courts: The privilege should not apply.

Contracts that do purport to block court-ordered disclosures are trickier. Stingrays are the most known but not the only example. Grayshift's competi-

335. United States v. Budziak, No. CR-08-00284, at 2 (N.D. Cal. Feb. 18, 2014), ECF No. 248 (protective order for defense review of the eP2P software); *see also* Notice of Motion & Motion to Compel Discovery; Points and Auths. (Rule 16(a)(1)(E) & Crim. Loc. Rule 16-2), United States v. Budziak, No. CR-08-00284 (N.D. Cal. Feb. 9, 2009), ECF No. 47.

336. United States v. Pirosko, No. 12-cr-00327, at 5 (N.D. Ohio Aug. 13, 2013), ECF No. 33 (order denying motion to compel).

337. United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. 2015).

338. *Our Work*, CHILD RESCUE COAL., https://childrescuecoalition.org/our-work [perma.cc/9PJV-92C3]; *see also Law Enforcement*, CHILD RESCUE COAL., https://childrescuecoalition.org/law-enforcement [perma.cc/P298-K3U7].

339. *See, e.g.*, 18 U.S.C. § 401.

340. *Magnet Graykey*, MAGNET FORENSICS, https://www.magnetforensics.com/products/magnet-graykey [perma.cc/CR42-7GAN].

341. *Grayshift, LLC End User License Terms*, MAGNET FORENSICS 3, https://www.magnetforensics.com/wp-content/uploads/2019/03/Grayshift_EULA-3.5.2018.pdf [perma.cc/PC49-GQNL]; *see also How to Get GrayKey from Magnet Forensics*, MAGNET FORENSICS (Feb. 19, 2019), https://www.magnetforensics.com/blog/how-to-get-graykey-from-magnet-forensics [perma.cc/JG3D-LBLA].

tor, Cellebrite, also sells hacking services to law enforcement to crack passwords and extract data from phones, tablets, computers, and cloud accounts.[342] Its contracts with police departments[343] say it will not disclose sources or methods in "any investigations, indictments, motions, hearings, trials, or any other form of judicial proceedings."[344] They also state that the company will refuse to comply with court-ordered disclosures for information other than chain of custody or data extracted from particular devices.[345] In this case, the contract effectively promises to assert privilege and thus enhances confidentiality in a manner that could support a privilege claim. At the same time, a court may find that a protective order can still offer stronger safeguards than the contractual nondisclosure agreement, which would support ordering disclosure.[346] Hence, claiming privilege could become more like a means of ensuring a strong protective order than a route to total nondisclosure.

One final note is in order. When courts review law enforcement secrets in camera, the government sometimes imposes onerous confidentiality requirements on the judge.[347] Papers might be delivered to a judge by a special agent handcuffed to their briefcase. The judge might be required to close the window shades before viewing documents. Alternately, the judge might have to travel

---

342. *General Terms and Conditions*, CELLEBRITE, https://legal.cellebrite.com/CB-us-us/index.html [perma.cc/RK7K-X2ET].

343. *See e.g.* Contract between City of Glendale and Cellbrite, Inc. (June 28, 2022), https://docs.glendaleaz.com/WebLink/DocView.aspx?id=7217408&dbid=0&repo=City-of-Glendale&cr&cr=1 [perma.cc/N8BS-F3YF] (contract between Cellebrite and a police department in Glendale, Arizona); Renewal of Contract between Wise County, Tex. and Cellebrite (July 12, 2024), https://www.co.wise.tx.us/DocumentCenter/View/567/Cellebrite---Renewal-PDF [perma.cc/24QM-BJHB]; Contract between City of Fort Worth, Tex. and Cellebrite (June 2, 2020), https://publicdocuments.fortworthtexas.gov/CSODOCS/DocView.aspx?id=212991&dbid=0&repo=City-Secretary&cr=1 [perma.cc/4CC3-77HH]; Contract between City of Lebanon, Mo. and Cellebrite (Nov. 23, 2020), https://www.lebanonmissouri.org/DocumentCenter/View/34336/Council-Bill-No-5088--Purchase-Cellebrite-Universal-Forensic-Extraction-Devices-Cellebrite [perma.cc/NC6S-AB6Y]; Contract between City of Inglewood. Cal. and Cellebrite (May 19, 2020), https://www.cityofinglewood.org/AgendaCenter/ViewFile/Item/9164?fileID=4432 [perma.cc/AXF8-TLF8]; Contract between Town of Davie, Fla. and Cellebrite (Feb. 5, 2019), https://www.davie-fl.gov/DocumentCenter/View/7415/NTSS-2019-33-Signed-Sole-Source?bidId= [perma.cc/J2DP-L6J4].

344. CELLEBRITE, *supra* note 342, at cl. 6.6.

345. *Id.* at cl. 6.6.3. The pertinent contractual provision states in full:

> In the event that Cellebrite is properly served with a subpoena seeking testimony concerning any Services, issued by a court of competent jurisdiction, then any testimony by Cellebrite personnel shall be limited to chain of custody issues concerning any Device on which Services have been provided and any Data extracted from any Device in connection with such Services.

Id.

346. *See, e.g.*, United States v. Newman, 531 F. Supp. 3d 181, 193 (D.D.C. 2021) ("[T]he appropriate course of action is for the parties to submit a joint motion for a protective order that will cover the documents subject to the confidentiality agreement . . . .").

347. *See generally* ROBERT TIMOTHY REAGAN, FED. JUD. CTR., KEEPING GOVERNMENT SECRETS: A POCKET GUIDE FOR JUDGES ON THE STATE-SECRETS PRIVILEGE, THE CLASSIFIED INFORMATION PROCEDURES ACT, AND COURT SECURITY OFFICERS (2007).

to a secure location to view the records. These types of requirements can intimidate a judge who is considering ordering disclosure. Knowing whether law enforcement has previously imposed the same conditions on its own officers could help judges distinguish genuine security concerns from security theater that might unduly sway their decisions.

C. *Critiques and Responses*

This Section considers predictable doubts about courts tying privilege claims to law enforcement's pre-dispute conduct and explains why these doubts should not dissuade courts from adopting the reform or legislators from imposing it.

1. Mismatch Scenarios

It should be clear that law enforcement's pre-dispute conduct will make a fine proxy for the value of secrecy when information is truly sensitive and law enforcement has imposed strict confidentiality, or when information is not truly sensitive and law enforcement has imposed lax confidentiality. The difficulty comes from the mismatch scenarios. What if information is very sensitive and yet, due to bad lawyering or sloppy governance, law enforcement has negligently failed to protect it? Think of scenarios like *Budziak*, in which the FBI failed to monitor copies of purportedly sensitive information possessed by a private contractor and its departing employees.[348]

There are a few responses. If law enforcement has negligently failed to protect truly sensitive information, then punishing them by ordering disclosure could encourage more responsible conduct in the future.[349] To be sure, courts might worry about applying such punitive logic if the officials who engaged in poor behavior will not internalize the costs,[350] and especially so if the public will instead accrue those costs.[351] Nonetheless, disclosure in litigation does not necessarily cost the public; it merely creates a *risk* that protective orders can mitigate. Setting disclosure as a default, rather than a mandatory rule, offers another case-by-case safety valve. Even if some judges depart from the default to maintain secrecy despite law enforcement's prior, sloppy conduct,

348. *See* United States' Response to Defendant's Motion for Discovery Remedy, *supra* note 151, at 4.

349. *Cf.* John C. Jeffries, Jr., *The Liability Rule for Constitutional Torts*, 99 VA. L. REV. 207, 242–43 (2013); Guy Rubinstein, *The Prosecutor-Oriented Exclusionary Rule*, 65 B.C. L. REV. 1755, 1757 (2024) ("In theory, the [Exclusionary Rule] is supposed to deter police officers from violating the Fourth Amendment, by warning them that the evidence they obtain may be inadmissible in court.").

350. *See* JOANNA SCHWARTZ, SHIELDED: HOW THE POLICE BECAME UNTOUCHABLE (2023); John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539, 1573 (2017).

351. *See, e.g.*, Dellwood Farms, Inc. v. Cargill, Inc., 128 F.3d 1122, 1127 (7th Cir. 1997).

this is not an area where judicial reticence to punish the government will stymie important innovation in the law, as excessive damages liability might do for constitutional rights.[352] And the potential for other judges to order disclosure in similar circumstances should still motivate law enforcement to be more careful moving forward.

Alternately, what if information is not truly sensitive, and law enforcement has unnecessarily secured it? Officers engaged in knowing fraud or misconduct already have incentives to conceal. Meanwhile, this Article's proposed reform could incentivize greater secrecy among well-meaning officers as well. Law enforcement agencies might respond to the reform by routinely making everything extra confidential.

Once again, there are a few responses. To start, law enforcement's conduct should set a floor, not a ceiling, for transparency. That is how most nongovernmental privileges and trade secret laws already work. One must show a reasonable expectation of confidentiality to claim the attorney-client, spousal, clergy-penitent, or psychotherapist-patient privilege. But doing so does not guarantee privilege protection.[353] So too, showing reasonable efforts to maintain secrecy is necessary but not sufficient for a trade secret claim.[354] Similar logic should apply to law enforcement secrecy.

Next, to the extent that law enforcement's institutional incentives lean toward secrecy, using law enforcement's pre-dispute conduct as a proxy will offer a conservative estimate of an acceptable risk of leaks. Courts should thus feel more confident about ordering disclosure under protective-order safeguards that match or exceed what law enforcement previously imposed. Of course, this practice may result in unnecessarily burdensome protective orders.[355] Even so, it would improve over the total nondisclosure that often happens today.

Meanwhile, maintaining confidentiality has costs of its own that will predictably discourage law enforcement from adopting excessive precautions. Maintaining confidentiality may require limiting the number of people who can use an investigative technique or otherwise constraining the circumstances of its use. It may present obstacles for collaboration between federal, state, local, tribal, and territorial law enforcement partners. It may require routine tracking of sensitive information, demanding the return or destruction of information following use, or independent investigations and disciplinary actions to enforce against unauthorized disclosures. Cumulatively, such costs could be substantial.

---

352. *See* Jeffries, *supra* note 349, at 247–48, 261; William J. Stuntz, *The Virtues and Vices of the Exclusionary Rule*, 20 HARV. J.L. & PUB. POL'Y 443 (1997).

353. *See, e.g.*, Imwinkelreid, *supra* note 320, at 4, 14.

354. *See supra* note 326 and accompanying text.

355. *Cf.* State v. Pickett, 246 A.3d, 279, 290–91 (N.J. Super. Ct. App. Div. 2021) (holding that a protective order making defendant's source code available for independent review was unnecessary where the state did not intend to review it).

Economics literature helps to explain the significance of such costs. According to economist Michael Spence, whether decisionmakers can rely on information (e.g., confidentiality conduct) as a signal for an unseen characteristic (e.g., truly sensitive investigative methods) depends on two traits.[356] To start, the signal itself should correlate positively with the unseen characteristic. Next, the cost of generating the signal should correlate negatively with the same unseen characteristic.[357] For courts assessing law enforcement privilege claims, law enforcement's pre-dispute confidentiality conduct has both traits. It correlates positively with truly sensitive investigative methods because such methods that are not kept confidential will be destroyed. Meanwhile, the cost *differential* for law enforcement to generate confidentiality increases as the sensitivity of the investigative method decreases: Any friction that confidentiality imposes on law enforcement operations will have fewer countervailing benefits for investigative methods that do not actually need secrecy to remain effective. Spence's theory thus suggests that confidentiality would be a reliable signal for courts, even as law enforcement may ex ante game its conduct in response to the judicial test.

Concededly, officers engaged in knowing fraud or misconduct present the most challenging case because these individuals will find ex ante secrecy so valuable. Whether evaluating their pre-dispute conduct will help judges depends on whether one thinks the individuals' incentives to lie will increase or decrease as litigation proceeds. If the incentives to lie will increase, then assessing their pre-dispute conduct will still be more reliable than their post-dispute testimony. If the incentives to lie will decrease, perhaps because the risk of punishment for perjury creates a successful deterrent, then this is the edge case where this Article's reform proposal will offer no benefit.

2. Judicial Incentives

Of course, not every judge will wring their hands at the thought that current doctrine creates an exceedingly vague or even conceptually limitless law enforcement secrecy power. On the contrary, the vagueness of current doctrine is judge-made and arguably reflects a variety of institutional incentives shared by many members of the judiciary. As Ana Lvovsky has articulated especially well, judges' motives for deferring to law enforcement are numerous and can include political pressures; personal ideological sympathies; pragmatic sensitivity to the challenges of policing; a desire to manage caseloads by simplifying or avoiding otherwise "sticky legal issues"; a preference for disposing of issues through "procedural lenience" towards the police rather than potentially "controversial or corrosive substantive holdings"; and a pull to

356. Michael Spence, *Signaling in Retrospect and the Informational Structure of Markets*, 92 AMER. ECON. REV. 434, 436–37 (2002).

357. *Id.* at 437.

maintain stable relationships with repeat government players in their courtrooms.[358] Further, some judges no doubt believe that comparative institutional competencies and judicial restraint counsel an overarching tilt toward noninterference with law enforcement practices.[359]

Each of these reasons may well help to account for the current state of law enforcement privilege doctrine. Vagueness in the doctrine provides cover for deference. Deference, in turn, enables judges to avoid uncomfortable and time-consuming decisions. By maintaining the secrecy of law enforcement techniques, courts make it less likely that defendants will expose borderline or indeterminate police investigative conduct that might raise complex factual inquiries, hard constitutional and legal questions, and ultimately require the suppression of probative evidence of guilt, including in prosecutions of very serious crimes. Put succinctly, secrecy can forestall entire lines of motion practice that would otherwise clog dockets and force difficult rulings.[360]

Nonetheless, it would be a mistake to conclude that there is no hope for judge-made doctrine to bound the law enforcement privilege more reasonably. Judges have a mix of institutional incentives, including pressures to protect the interests of criminal defendants.[361] Secrecy concerning law enforcement investigative techniques does not entirely eliminate docket-clogging motions or thorny legal and constitutional issues. Those that remain still present time-consuming battles of the experts; they are simply less informed. Perhaps most significant, even a single judge adopting the proposed reform and ordering disclosure could produce widespread benefits for both police accountability and investigative accuracy. Even if investigative methods are disclosed under a strict protective order, the judge's conclusions as to their lawfulness and reliability need not be. Regardless of the overarching institutional incentives of the judiciary, some individual judges will wish to engage in a more probing review of law enforcement secrecy claims. This Article's proposal should help those judges.

3. Downstream Disclosures

Finally, some readers may worry about the downstream effects of a doctrine that presumes in-court disclosures will occur under protective orders. Admittedly, protective orders can create problems of their own. On the one hand, they can obstruct important information flows. For instance, police departments' internal misconduct records revealed under a protective order in one case may constitute *Brady* material in another, but the protective order may impede prosecutors in the first case from disclosing the information in

358. Lvovsky, *supra* note 65, at 2053–55.

359. Lvovsky, *supra* note 124, at 491–92.

360. *Cf.* Aziz Z. Huq, *Judicial Independence and the Rationing of Constitutional Remedies*, 65 DUKE L.J. 1, 67–68 (2015).

361. *See* William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 540–42 (2001).

the second.[362] Protective orders can also keep the public from learning about police misconduct.[363] On the other hand, protective orders offer imperfect secrecy protections. Even setting aside the risk of leaks, once evidence is admitted at trial, a host of other access rights come into play that may cause courts to lift the protective order. For example, protective orders can conflict with Sixth Amendment public trial rights.[364] Also, information disclosed under a protective order that ultimately forms the basis of a judicial decision will trigger the public's common-law and First Amendment rights of access to courts.[365] Third-party intervenors can then move to unseal and publish the records to the public.

The response to this objection is simple: Whether protective orders should yield to follow-on disclosure needs is a separate determination with its own standards for judgment.[366] Courts should not mix and match their reasoning by allowing speculation about future disclosure needs to contaminate the threshold inquiry of whether a privilege has been legitimately invoked.

CONCLUSION

Judge José A. Cabranes writing for the United States Court of Appeals for the Second Circuit aptly described the conundrum at the heart of this Article: "It is hard to imagine, therefore, many 'question[s] of law' that carry greater 'significan[ce]' than the question of when the goals of the law enforcement privilege must give way to a party's need for discovery."[367]

This Article has explained how the law enforcement privilege can obstruct police accountability and lead to wrongful convictions while acknowledging that, in some cases, it serves important policy goals in effective investigative methods. The Article teased out what minimal rules exist to cabin the privilege in current federal appellate doctrine and identified a core problem with those rules: In a subtle conceptual collapse, courts are mistakenly using the privilege's policy rationale as the test for assessing threshold claims to privilege. That rationale is too vague to create a meaningful constraint.

---

362. Jonathan Abel, Brady*'s Blind Spot: Impeachment Evidence in Police Personnel Files and the Battle Splitting the Prosecution Team*, 67 STAN. L. REV. 743, 802–03 (2015).

363. Chelsea Hanlock, Note, *Settling for Silence: How Police Exploit Protective Orders*, 109 CALIF. L. REV. 1507 (2021).

364. *See, e.g.*, Kristin Saetveit, Note, *Close Calls: Defining Courtroom Closures Under the Sixth Amendment*, 68 STAN. L. REV. 897, 909–19, 922–32 (2016).

365. *See In re* Leopold to Unseal Certain Elec. Surveillance Applications and Orders, 964 F.3d 1121, 1126–27 (D.C. Cir. 2020) (refusing to reach the constitutional question when a journalist appealed a district court's denial to unseal certain judicial records on both First Amendment and common-law rights of access grounds); *cf.* Diego A. Zambrano, *Missing Discovery in Lawyerless Courts*, 122 COLUM. L. REV. 1423, 1461–62 (2022).

366. *See In re Leopold*, 964 F.3d at 1127.

367. *In re* City of New York, 607 F.3d 923, 942 (2d Cir. 2010) (alterations in original) (quoting *In re* SEC *ex rel.* Glotzer, 374 F.3d 184, 187 (2d Cir. 2004)).

After providing this positive account of the law enforcement privilege and its problems, the Article turned normative. To lay the groundwork for a reasoned reform proposal, it initially debunked the current scholarly consensus that no privilege for law enforcement methods existed at common law. The erroneous view that the privilege is ahistorical mystifies the challenges of reforming what is in fact longstanding and entrenched. Next, the Article considered existing proposals to abolish the privilege, either entirely or for information possessed by private entities. Neither proposal withstands serious scrutiny.

Instead, the Article argued that courts should evaluate privilege claims by reference to the marginal risk of *leaking* posed by in-court disclosure. To do this, judges should assess how law enforcement itself previously treated the purportedly privileged information. If the safeguards available through a court-ordered protective order could match or exceed law enforcement's own prior confidentiality requirements, courts should default to ordering disclosure. This approach has substantive, institutional, procedural, and normative advantages. Though the approach deviates substantially from current appellate requirements, it has precedents in other areas of secrecy law and literature.

More generally, this Article's analysis suggests a new "circumstantial evidence" theory of confidentiality's role in privilege law as a whole, with potentially radical implications for government privilege writ large. Most *non*-government privileges that shield communications between two parties—such as the attorney-client, spousal, or psychotherapist-patient privileges—require claimants to establish a reasonable expectation of confidentiality in the allegedly privileged information. The standard explanation for this requirement is a utilitarian story about incentives. John Henry Wigmore, arguably the most influential evidence scholar of all time, thought that expectations of confidentiality incentivized people in certain relationships to communicate.[368] He reasoned that privileges should apply only to communications that would not occur but for this incentive or, in his words, to communications that "originate in a confidence that they will not be disclosed."[369] That way, privileges could be characterized as cost-free to the courts, suppressing only evidence that would not otherwise exist.[370]

But the incentives explanation is harder to buy for the many government privileges that shield topical information, such as law enforcement investigative methods; official records; or national security, military, and diplomatic secrets. Topical privileges do not always involve a person whose communications can be incentivized. Hence, the standard theory has left government privileges adrift. Unsurprisingly, the law enforcement privilege is not the only

368. *See, e.g.*, Imwinkelried, *supra* note 321, at 319–20.

369. 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2285 (McNaughton rev. 1961) (emphasis omitted).

370. *See, e.g.*, Imwinkelried, *supra* note 321, at 319–20.

government privilege where current doctrine fails to factor pre-dispute confidentiality into the test for assessing a threshold claim.[371] Indeed, just recently in *United States v. Zubaydah*, a case in which a torture survivor sought to compel testimony from the CIA contractors who orchestrated his torture, the Supreme Court doubled down on the government's right to claim the state secrets privilege even for information that has been widely disseminated in the press.[372]

This Article has offered an alternative "circumstantial evidence" rationale for confidentiality requirements that applies as easily to topical as to communications privileges: A privilege claimant's pre-dispute conduct concerning the confidentiality of information offers circumstantial evidence of the value of keeping that information secret. The evidence is especially useful because it is likely more reliable than post-dispute testimony, it leverages the claimant's own expertise to assist in judicial review, and it can be adjudicated publicly in a fully adversarial hearing without revealing the actual contents of the purportedly privileged information. None of this reasoning need be limited to the law enforcement privilege alone. The issue of adding confidentiality requirements to constrain other government secrecy powers is thus ripe for further scholarly contribution.

371. *See* 26 WRIGHT, GRAHAM & MURPHY, *supra* note 72, §§ 5661–72; 26A WRIGHT, GRAHAM & MURPHY, *supra* note 72, §§ 5673–82.

372. Chesney, *No Appetite*, *supra* note 68.