COOPTING PRIVACY

CHRISTINA KONINGISOR*

Privacy law in the United States is sectoral in nature. And at every turn, it privileges the police. On the front end, privacy statutes uniformly exempt law enforcement agencies, allowing police to gather private information when access is denied to other government and private actors. And on the back end, public records laws contain myriad privacy carveouts that police use as a pretext to shield their activities from public view.

The many privileges granted to law enforcement agencies when accessing private information have been documented by legal scholars. But there has been less attention paid to the powerful secrecy protections extended to police in the name of privacy. This Article examines these privacy-focused provisions and the tensions and trade-offs they entail. It maps these privacy claims across different substantive contexts. And it argues that police too often weaponize these privacy protections to shield themselves against public scrutiny. Privacy protections become coopted by police to serve anti-accountability ends.

This cooption introduces three related harms. First, the current legal regime privileges protection against certain types of privacy intrusions, such as those imposed by the public dissemination of private information, at the expense of others, such as those imposed by government data collection and processing. Second, it encodes within the information-access regime a set of distributive choices that favor powerful groups at the expense of marginalized communities. And third, it imposes substantial democratic costs, often without any corresponding privacy benefits.

* Associate Professor of Law, U.C. College of the Law, San Francisco (formerly U.C. Hastings). Many thanks to Emmanuel Arnaud, Marc Blitz, Bridget Dooling, Yan Fang, Christine Kim, Margaret Kwoka, Irina Manta, Catherine Powell, Daniel Solove, Miriam Seifter, Alicia Solow-Niederman, Jacob Noti-Victor, Ari Ezra Waldman, Jordan Wallace-Wolf, and Felix Wu, as well as to participants in the 2023 Privacy Law Scholars Conference, the 2023 University of Wisconsin State Democracy Research Initiative's State Constitutional Law Roundtable, the 2024 Rocky Mountain Junior Scholars' Conference, Cardozo Law School's Intellectual Property and Information Law Colloquium, Ohio State's Information Governance Colloquium, and the faculty workshop at George Washington Law School. Many thanks as well to the Berkeley Center for Law and Technology for supporting this research. My deepest gratitude to my excellent research assistants Alexander Wilson McFarlin, Julia Ivory, and Jensen Lillquist.

CONTENTS

INTRODUCTION

Early in the morning on March 23, 2020, police officers in Rochester, New York, arrested Daniel Prude, an unarmed Black man with a history of mental health issues.[1] They placed a hood over his head and violently restrained him on the ground. Prude died of his injuries a week later.[2]

In the weeks following Prude's death, his family submitted a request under the state's freedom of information law for body camera footage of the incident.[3] Emails later revealed that police and city officials had strategized at length about how to keep the video secret. "I'm wondering if we shouldn't hold back on this for a little while considering what is going on around the country," one police officer wrote.[4] "Can we deny/delay?" a lawyer for the city asked.[5] Another argued that if the tape were released, the "City will burn" and "we will all lose our jobs."[6]

In the following months, the city raised various objections to disclosure, often on shaky legal grounds.[7] These claims included the assertion that the city was obligated to withhold the body camera footage to protect Prude's own privacy interests. City officials argued that handing over the video to Prude's family would violate Prude's medical privacy rights. And they required the family to sign a notarized release under the Health Insurance Portability and Accountability Act ("HIPAA"), the federal law that addresses patient privacy,[8] even though HIPAA doesn't apply to law enforcement agencies.[9] City officials later admitted that they knew the signed release was not required by law, but

[1] Michael Gold & Troy Closson, *What We Know About Daniel Prude's Case and Death*, N.Y. TIMES (Apr. 16, 2021), https://www.nytimes.com/article/what-happened-daniel-prude.html.

[2] *Id.*

[3] ANDREW G. CELLI, JR., KATHERINE ROSENFELD, SCOUT KATOVITCH, KATHRYN RAVEY & JOCELYN RODRIGUEZ, INDEPENDENT INVESTIGATION OF THE CITY OF ROCHESTER'S RESPONSE TO THE DEATH OF DANIEL PRUDE 32 (2021), https://ecbawm.com/wp-content/uploads/2021/03/Final-Report-of-the-Independent-Investigation-of-the-City-of-Rochesters-Response-to-the-Death-of-Daniel-Prude-issued-March-12-2021-00452102x9CCC2.pdf [https://perma.cc/GP7E-XL5U].

[4] *Id*.

[5] Hannah Knowles & Marisa Iati, *No Officers Indicted in Death of Daniel Prude, a Black Man Pinned and Hooded During Mental Crisis*, WASH. POST (Feb. 23, 2021), https://www.washingtonpost.com/nation/2021/02/23/daniel-prude-rochester-death-officers/.

[6] CELLI ET AL., *supra* note 3, at 14.

[7] *Id*. at 14, 31-32 (describing various delay tactics employed by city).

[8] *Id.* at 34.

[9] *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-9.

they asked for it anyway.[10] By the time the family returned the HIPAA form, the city had extended its monthslong delay in releasing the footage even further.[11]

Government actors, especially law enforcement agencies, routinely utilize privacy interests to serve their own ends. In recent decades, citizens have struck an implicit bargain with federal, state, and local governments. Under the current privacy law regime, law enforcement agencies are permitted to collect large volumes of data about their citizens.[12] In exchange, the government is granted broad secrecy powers to guard this information against further public dissemination.[13] Under this arrangement—limited ex ante restrictions on police data collection, combined with expansive ex post privacy protections against broader public disclosure—law enforcement agencies receive significant access to and control over privileged information.

The first prong of this regime—limited restrictions on police information gathering—can be seen in the myriad law enforcement exceptions contained in privacy statutes. The federal statutory privacy regime is largely sectoral in nature. There are separate statutes shielding medical records, home video rental records, educational records, and more from disclosure to either public or private actors.[14] But these statutes share a common feature: Each contains an exception permitting law enforcement actors to access the data.[15] A growing number of

[10] *See* CELLI ET AL., *supra* note 3, at 10.

[11] *Id.*

[12] *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 503 (2013) (describing how law enforcement agencies are uniformly exempt from privacy protections imposed by sectoral privacy laws and concluding "law enforcement is the sole interest consistently exempted from general provisions").

[13] This arrangement is largely embodied in two related sets of statutes: federal and state public records laws like The Freedom of Information Act ("FOIA"); and federal and state privacy laws, like Certificates of Public Advantage ("COPA") and HIPAA. *See infra* note 26 and accompanying text.

[14] For a summary of the sectoral nature of this federal regime, see, for example, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 906-13, 916-21 (2009). States, in contrast, have enacted comprehensive privacy statutes. *See* discussion *infra* note 55 and accompanying text.

[15] *See, e.g.*, Fanna Gamal, *The Private Life of Education*, 75 STAN. L. REV. 1315, 1324-25 (2023) (describing law enforcement exceptions to privacy protections for educational records); Murphy, *supra* note 12, at 487 (noting "across this remarkable diversity" in information privacy statutes, "there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms"); Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212, 229 (2021) (noting many information privacy statutes "include express textual exceptions that authorize disclosures to law enforcement").

states have also enacted comprehensive consumer privacy laws.[16] These state laws, too, provide sweeping carve outs for law enforcement.[17] Taken together, this patchwork of federal and state privacy laws provide only limited protections against police intrusion.[18]

The second prong of this information-access regime—powerful back-end privacy protections against broader public disclosure of information held by the police—is largely embodied in federal and state transparency laws.[19] Every state has a public records law requiring the release of certain records to the public upon request, analogous to the federal Freedom of Information Act ("FOIA").[20] Under these statutes, government records are presumptively open. They may be withheld only if they fall within one of a series of enumerated exemptions.[21] These exemptions differ from one jurisdiction to the next. Yet every statute protects private information from public disclosure in some form.[22]

Law enforcement agencies receive special treatment under these transparency laws as well. Legislatures grant police extensive statutory carveouts.[23] Judges develop FOIA-specific doctrines that favor law enforcement interests.[24] And law enforcement agencies interpret these exemptions in ways that expand their scope

[16] *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L., https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/ (last updated Apr. 7, 2025) (explaining that twenty states currently have comprehensive data privacy laws in place).

[17] *See, e.g.*, CAL. CIV. CODE § 1798.145(a)(1)(B) (West 2025) (creating law enforcement exemption to state's consumer privacy act); COLO. REV. STAT. § 6-1-1304(3)(a)(III) (2025) (same); CONN. GEN. STAT. ANN. § 42-529d(c)(3) (West 2025) (same); N.J. STAT. ANN. § 56:8-166.15(3) (West 2025) (same); UTAH CODE ANN. § 13-61-304(1)(c) (LexisNexis 2025) (same).

[18] *See* sources cited *supra* note 15. Of course, there are important constitutional provisions limiting law enforcement investigatory powers. But these, too, suffer from substantial exceptions and flaws. The work addressing the many dimensions of this problem is voluminous. *See, e.g.*, David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1071 (2014) (describing "doctrinal disarray" in Fourth Amendment privacy law); William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1267 (1999) (describing distributive harms embedded in Fourth Amendment doctrine).

[19] The Freedom of Information Act contains expansive carveouts from disclosure for police records. *See* 5 U.S.C. § 552(b)(7) (describing five subcategories of protected law enforcement records). Virtually every state public records law contains similar carveouts. For a summary, see Christina Koningisor, *Police Secrecy Exceptionalism*, 123 COLUM. L. REV. 615, 640-41 (2023).

[20] 5 U.S.C. § 552.

[21] *Id.* § 552(b)(1)-(9) (detailing subcategories of exemptions).

[22] *See supra* note 19.

[23] Koningsor, *supra* note 19, at 637.

[24] *Id.* at 651-55.

of protections from the bottom up.[25] As a result, police end up twice-privileged under the current information-access regime. They receive broader front-end access to gather information than other private or government actors. And they also receive more powerful back-end privacy protections to shield this sensitive information from public view.

The first component in this dynamic—the data-gathering privileges granted to police under federal and state privacy statutes—has been explored by legal scholars. Professors Erin Murphy, Sunita Patel, Rebecca Wexler, and others have chronicled how the statutory privacy regime favors law enforcement and grants police access to information that is denied to other criminal justice actors, especially criminal defendants.[26] Yet the second step—the privacy privileges granted to police under state constitutions and transparency laws—has received less attention. Transparency and criminal law scholars have examined the role of privacy concerns in shielding certain categories of records, especially police disciplinary records and body camera footage, from disclosure.[27] But this

[25] *Id.* at 655-62 ("These secrecy-enhancing efforts . . . take a variety of forms, including construing these exemptions broadly at the administrative level, inserting information-protective provisions in police contracts, refusing to gather information and create records, and ignoring the requirements of the law altogether.").

[26] *See, e.g.*, Murphy, *supra* note 12, at 487; Sunita Patel, *Transinstitutional Policing*, 137 HARV. L. REV. 808, 874-82 (2024); Wexler, *supra* note 15, at 229. Scholars have also explored the various harms that flow from the loss of privacy elicited by police data-gathering efforts. *See, e.g.*, Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205, 209 (2021) (describing how police data is being "mined, manipulated, and studied by powerful computer analytics" to be used in criminal prosecutions); Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1150-52 (2022) (describing breadth of police data gathering efforts); Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. 2007, 2024-31 (2022) (describing how carceral sources of knowledge are infected with racial and socioeconomic bias).

[27] For work exploring the intersection between privacy interests and public access to police body-worn cameras, see, e.g., Cynthia H. Conti-Cook, *Open Data Policing*, 106 GEO. L.J. ONLINE 1, 6 (2017), https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/conti-cook-open-data-policing_ACCESSIBLE.pdf [https://perma.cc/HMX9-S6Q7]; Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 400 (2016); Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1261 (2018); Kami Chavis Simmons, *Body-Mounted Police Cameras: A Primer on Police Accountability vs. Privacy*, 58 HOW. L.J. 881, 889 (2015); and Tolulope Sogade, *Body-Worn Camera Footage Retention and Release: Developing an Intermediate Framework for Public Access in a New Affirmative Disclosure-Driven Transparency Movement*, 122 COLUM. L. REV. 1729, 1757 (2022). For work exploring the intersection between privacy interests and public access to police disciplinary records, see, e.g., Kevin M. Keenan & Samuel Walker, *An Impediment to Police Accountability? An Analysis of Statutory Law Enforcement Officers' Bills of Rights*, 14 B.U. PUB. INT. L.J. 185, 187-88 (2005); Kate Levine, *Discipline and Policing*, 68 DUKE L.J. 839, 872-80 (2019); and Rachel Moran, *Police Privacy*, 10 U.C. IRVINE L. REV. 153, 156 (2019).

broader privacy regime, encompassing the full set of police privacy shields embedded in these state transparency laws, remains underexplored.

Privacy law scholars have examined the problem of the pretextual use of privacy interests.[28] Yet much of this work is focused on privacy intrusions imposed by the private sector.[29] There has been less attention paid to the cooption of privacy interests by government actors, including police.[30]

For more general discussions of the "administrative turn" in police scholarship, see, e.g., Kenneth Culp Davis, *An Approach to Legal Control of the Police*, 52 TEX. L. REV. 703, 704 (1974); Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1848-50 (2015); Rachel Harmon, *Why Do We (Still) Lack Data on Policing?*, 96 MARQ. L. REV. 1119, 1128-32 (2013); and Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 93 (2016).

[28] *See, e.g.*, Nadia Banteka, *Unconstitutional Police Pretexts*, 2023 WIS. L. REV. 1871, 1975-77 (linking permissibility of police privacy pretexts in Fourth Amendment context to police privacy pretexts in other, related legal contexts); Susan Hazeldean, *Privacy as Pretext*, 104 CORNELL L. REV. 1719, 1721 (2019) (arguing privacy claims have been used as pretext to discriminate against transgender people); Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951, 971 (2021) (describing how platforms invoke users' privacy interests against competitors while simultaneously selling that same user data itself); Neil Richards, *The GDPR as Privacy Pretext and the Problem of Co-Opting Privacy*, 73 HASTINGS L.J. 1511, 1523-36 (2022) (describing how companies invoke GDPR as pretext to evade U.S. discovery obligations in transnational litigation); Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1631 (2019) [hereinafter Van Loo, *The Missing Regulatory State*] (exploring how privacy interests are used by platform companies as pretext for deregulatory efforts); Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 101, 103 (2022) [hereinafter Van Loo, *Privacy Pretexts*] (arguing that businesses have been coopting privacy claims to protect their own business interests); Wexler, *supra* note 15, at 2722 (exploring how tech companies invoke privacy interests to shield information from criminal defendants); *see also* AMY GAJDA, SEEK AND HIDE: THE TANGLED HISTORY OF THE RIGHT TO PRIVACY 255 (2022) (examining more generally ways privacy interests can be used by powerful political actors as anti-accountability mechanism).

[29] *See, e.g.*, Kadri, *supra* note 28, at 971; Richards, *supra* note 28, at 1523-36; Van Loo, *Privacy Pretexts*, *supra* note 28, at 103; Van Loo, *The Missing Regulatory State*, *supra* note 28, at 1631; Wexler, *supra* note 15, at 2722.

[30] *See* Richards, *supra* note 28, at 1513 ("The story of how powerful entities co-opt privacy is . . . growing, but the picture remains incomplete."). There are important exceptions. *See, e.g.*, Banteka, *supra* note 28, at 1892-904 (examining police pretexts across various substantive contexts, including pretextual use of privacy statutes); Amy L. Stein, *Domestic Emergency Pretexts*, 98 IND. L.J. 479, 484 (2023) (examining executive branch's pretextual use of emergency declarations to serve other ends). Legal scholars have also examined the privacy-accountability trade-offs embedded within transparency statutes more generally. *See, e.g.*, James Jacobs & Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 211-12 (2008) (describing accountability benefits versus privacy harms of criminal records databases); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1138

Scholars have also examined police privacy intrusions more broadly, and the harms that they impose in the criminal justice context. Legal scholars, criminologists, sociologists, political scientists, and more have explored many different aspects of privacy and policing. This body of work is rich and multifaceted, and it stretches back decades.[31] Yet much of it focuses on the first-order privacy harms imposed by police data collection. There has been less attention paid to the second-order harms introduced when the government deploys these extensive privacy shields as a mechanism to evade public oversight and accountability.[32]

This Article begins this work. Part I maps out the constitutional and statutory privacy carveouts granted to government agencies, especially law enforcement agencies. In doing so, it illuminates two central categories of police privacy protections: those intended to shield the privacy of police officers; and those

(2002) (describing privacy harms imposed by failing to adequately protect private information collected for government records). In the specific context of policing, much of this work has focused on the privacy implications of releasing body-worn camera footage and access to police disciplinary records. *See* sources cited *supra* note 27.

[31] This body of work is too extensive to map out in full here. For some recent examples, see, SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING (2020) (chronicling how police are using surveillance technologies and big data tools); KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017) (demonstrating various ways that women receive reduced privacy rights and protections); BRYCE CLAYTON NEWELL, POLICE VISIBILITY: PRIVACY, SURVEILLANCE, AND THE FALSE PROMISE OF BODY-WORN CAMERAS (2021) (conducting empirical research into how police officers manage new "information politics" of body camera surveillance); ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) (describing how algorithm-driven policing is affecting both law enforcement agencies and the public); SARAH A. SEO, POLICING THE OPEN ROAD: HOW CARS TRANSFORMED AMERICAN FREEDOM (2021) (describing how expansion of police automobile searches fueled a broader rise in policing and a loss in public privacy); Chaz Arnett, *From Decarceration to E-Carceration*, 41 CARDOZO L. REV. 641 (2019) (describing privacy, liberty, and democratic participation harms imposed by electronic surveillance in criminal justice system); I. Bennett Capers, *Criminal Procedure and the Good Citizen*, 118 COLUM. L. REV. 653, 655 (2018) (describing how Fourth Amendment case law is replete with assumptions about how a "good citizen" will "welcome[] police surveillance"); Devon W. Carbado, *Stop-and-Strip Violence: The Doctrinal Migrations of Reasonable Suspicion*, 55 HARV. C.R.-C.L. L. REV. 467, 467-81 (2020) (describing substantial bodily privacy intrusions imposed by "stop and strip" law enforcement searches); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 38 (2014) (critiquing failure of Fourth Amendment to constrain big-data policing); Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 115 (2017) (describing discriminatory impacts of big-data policing); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1017 (1995) ("[M]uch of what the modern state does *outside* of ordinary criminal investigation intrudes on privacy just as much as the kinds of police conduct that Fourth and Fifth Amendment law forbid.").

[32] For a discussion of exceptions, and some examples where scholars have begun the work of examining privacy-accountability tensions in policing, see *supra* note 30.

intended to protect the privacy of the public at large. Taken together, these two strands of privacy exemptions grant police substantial levels of informational protection.

Part II chronicles the ways that privacy interests facilitate police secrecy power. It examines examples of the pretextual use of privacy protections by police to achieve anti-accountability goals. And it argues that privacy concerns are too easily invoked as a shield to protect police departments from unwanted public oversight and scrutiny. Too often, privacy concerns operate as an unjustified mechanism of police secrecy.[33]

Part III examines the consequences of privacy cooption. Cataloguing this police privacy infrastructure brings at least three categories of harms into view. First, illuminating the police privacy regime brings various privacy-related tensions and tradeoffs to light.[34] The Article utilizes Professor Daniel Solove's taxonomy of privacy intrusions to flesh out the ways that the current information regime undervalues certain types of privacy harms.[35] Specifically, the current legal approach provides substantial protection against the privacy harms imposed by public disclosure. Yet it offers reduced safeguards against police data collection, data aggregation, and the secondary uses of private data, even though these latter harms are distinct.

Second, the current information-access regime embodies a set of distributive costs that privilege powerful groups at the expense of marginalized communities. Law enforcement agencies have expansive authority to shield information on privacy grounds. But this power is not distributed equally. Rather, it is deployed to protect certain groups over others—including police officers and other institutional actors whose interests align with police, such as gun owners.[36] In contrast, the records of those accused or convicted of crimes are largely open to public disclosure.[37] The Article maps out the infrastructure of police privacy, bringing these distributive effects into view. It also contributes to a growing body of work examining the subordinating effects of government data collection and other privacy intrusions.[38]

---

[33] The definition of privacy versus secrecy, and the terms of the relationship between the two, is complex. *See generally* Carol Warren & Barbara Laslett, *Privacy and Secrecy: A Conceptual Comparison*, J. SOC. ISSUES, Summer 1977, at 43, 44. For the purposes of this paper, I generally refer to privacy as an interest held by individuals and secrecy as a mechanism by which the government withholds information from the public.

[34] *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 222 (2016) (discussing how expanding privacy on one margin may contract it on another).

[35] *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490 (2006) (laying out four categories of privacy intrusions).

[36] At least thirty-three states explicitly exempt gun permit data from public disclosure. *See infra* note 326 (listing these statutory exemptions).

[37] *See* Levine, *supra* note 27, at 889 ("Unlike the police, who are well protected by their unions and legislators, criminal defendants and the formerly incarcerated have long suffered the fate of record publication.").

[38] For a discussion of this work, see *infra* note 318.

Third, pretextual privacy claims impose democratic harms. They prevent public oversight of government without any real privacy benefits. They also make it more difficult for the public to work through democratic channels to curtail police power. For example, police routinely invoke privacy concerns to shield information about programmatic surveillance efforts, often on flimsy doctrinal and theoretical grounds.[39] This makes it more difficult for citizens to understand and oppose these surveillance programs. And it feeds into a cycle of secrecy: the more information the police ingest through mass surveillance efforts, the more persuasive their anti-disclosure arguments become.

Part IV concludes with a discussion of possible remedies. It examines possible mechanisms for both reining in the problem of police privacy cooption and for reducing police data collection.

I. PRIVACY IN POLICE RECORDS

Law enforcement agencies have substantial privacy protections at their disposal to shield police records from public view. State constitutional provisions provide broad-based privacy shields. Privacy statutes contain myriad carveouts for law enforcement agencies. And federal and state public records laws provide various exemptions for private information contained in government records. This Part maps out this privacy regime for police records.

A. *General Privacy Protections*

1. Constitutional Protections

The federal Constitution contains important privacy protections against government overreach, especially those embodied in the Fourth Amendment.[40] Yet the U.S. Constitution never mentions the word "privacy."[41] And these provisions largely operate as an ex ante check against government data collection.[42] The Constitution has little to say about how private information is protected once it has been gathered by government officials, including law enforcement agencies.[43]

[39] *See* discussion *infra* Section II.B.

[40] U.S. CONST. amend. IV.

[41] *See generally* U.S. CONST.

[42] The Fourth Amendment's reasonable suspicion requirement also focuses largely on discrete pieces of information, what Professor Andrew Ferguson has referred to as a "small data doctrine." Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 338 (2015).

[43] There are exceptions. *See, e.g.*, State *ex rel.* Cincinnati Enquirer v. Craig, 132 Ohio St. 3d 68, 2012-Ohio-1999, 969 N.E.2d 243, at ¶ 13 (2012) (holding federal constitutional privacy protections shielded names of offices wounded in shoot-out from public view).

Some state constitutions, in contrast, contain more explicit privacy protections.[44] Florida's Constitution, for example, provides that "[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life."[45] Alaska's stipulates that "[t]he right of the people to privacy is recognized and shall not be infringed."[46] And New Hampshire's provides that "[a]n individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent."[47] Nearly a dozen state constitutions contain an express privacy provision.[48] And many additional state constitutions provide narrower privacy protections for more specific categories of people or records—crime victims' records,[49] for instance, or records relating to the voting process.[50]

These state constitutional privacy provisions can play an important role in resolving information disputes, especially in the context of policing.[51] Sometimes this treatment is explicit. California's constitutional privacy clause, for example, singles out the personnel files of certain law enforcement officers for protection.[52] More often, however, generalized constitutional privacy protections are applied in ways that privilege the privacy interests of the police.[53]

---

[44] *See* State Law Comparisons Spreadsheet (on file with author) (listing state constitutional privacy provisions).

[45] FLA. CONST. art. I, § 23.

[46] ALASKA CONST. art. I, § 22.

[47] N.H. CONST. art. 2-b.

[48] *See* ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, § 6; ILL. CONST. art. 1, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; N.H. CONST. art. 2-b; S.C. CONST. art I, § 10; WASH. CONST. art. I, § 7. A few of these clauses are embedded within broader state-level protections against unreasonable searches or seizures. *See* ILL. CONST. art. 1, § 6; LA. CONST. art. I, § 5; S.C. CONST. art I, § 10. But others operate as standalone privacy shields.

[49] *See* CAL. CONST. art. I, § 28(b)(1) (protecting "respect" for crime victim's "privacy"); IDAHO CONST. art. I, § 22(1) (guaranteeing crime victims treated with "privacy"); ILL. CONST. art. I, § 8.1(a)(1)-(2); KY. CONST. § 26A; OHIO CONST. art. I, § 10a(A)(1)-(2); OKLA. CONST. art. II, § 34; N.D. CONST. art. I, § 25(e)-(f); NEV. CONST. art. I, § 8A(1)(a); S.D. CONST. art. VI, § 29(5)-(6); WIS. CONST. art. I, § 9m(2b).

[50] *See, e.g.*, ARK. CONST. amend. 51, § 6 (requiring voter registration records be kept confidential).

[51] *See, e.g.*, City of Tallahassee v. Fla. Police Benevolent Ass'n, Inc., 375 So. 3d 178, 181 (Fla. 2023) (determining applicability of state constitutional privacy protections in context of police officer privacy); *see also* Mary Ellen Roy, *Louisiana: Open Government Guide*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/open-government-guide/louisiana/ [https://perma.cc/CPD8-335E] (last updated July 2023) ("More often than in the past, Louisiana courts are applying the elastic notion of constitutional 'privacy' to defeat records requests.").

[52] CAL. CONST. art. I, § 3(b)(3) (specifying the state's constitutional right of access provision does not abridge statutory protections for "information concerning the official performance or professional qualifications of a peace officer").

[53] *See* discussion *infra* Part II.B.2.

Taken together, these various constitutional privacy protections can operate as a significant source of police secrecy power.

2. Statutory Protections

The more common mechanism for protecting citizens' informational privacy rights is by federal or state statute. This category includes sectoral privacy laws that protect certain categories of sensitive information from being accessed by public or private actors. It also includes generalized privacy exemptions to transparency statutes, including public records laws.

a. *Privacy Laws*

Privacy law in the United States is mostly piecemeal and sectoral rather than transsubstantive. While other countries have passed comprehensive privacy legislation, the United States has taken a more decentralized approach, at least at the federal level.[54] A growing number of state legislatures have passed sweeping data protection laws.[55] And Congress has enacted an array of subject-specific laws to shield specific categories of data and information.[56] But there is no omnibus federal privacy statute. Instead, citizen records are largely governed at the federal level by subject-specific laws that protect certain categories of information.[57]

What unites these subject-specific laws is that virtually all of them permit access by law enforcement agencies.[58] One study of over twenty federal privacy statutes found that law enforcement "is the sole interest consistently exempted from general provisions."[59] Further, law enforcement agencies play a central role not just in crafting these privacy carveouts, but also in shaping the laws

[54] *Compare* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) 33 (EU), *with* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1632 (1999) (noting United States generally lacks comprehensive federal privacy laws and mostly regulates privacy one industry at a time).

[55] *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2025); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to -1314 (2025); 2021 Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -584 (2024). For a full list, see *Which States Have Consumer Data Privacy Laws?*, *supra* note 16.

[56] For a list of "major" privacy statutes as of 2013, see Murphy, *supra* note 12, at 546.

[57] *See id.* For a defense of this piecemeal, "sensitivity-focused" approach, see Paul Ohm, *Focusing Privacy Law*, BERKELEY TECH. L.J. (forthcoming 2025) (on file with author) (advocating benefits of narrower, sensitivity- and use-focused privacy laws).

[58] *See* Murphy, *supra* note 12, at 487. Other federal statutes impose privacy obligations that more squarely bind government entities. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (protecting against disclosure of personally identifiable information held by federal agencies).

[59] Murphy, *supra* note 12, at 503.

themselves through lobbying efforts.[60] The scope and structure of these ex ante privacy laws are inextricably intertwined with police priorities and preferences. And the pervasive exemptions contained in these privacy statutes allow police to gather especially sensitive information.[61]

b. *Transparency Laws*

In addition to these front-end protections against the collection of private data, federal and state legislatures have also enacted statutory protections against the back-end dissemination of private information already gathered by government. Specifically, FOIA and the fifty state public records laws extend privacy shields for information contained in government records.[62] Yet while such privacy protections appear in every federal and state public records law, they take different forms across different jurisdictions.

At the federal level, FOIA contains a centralized and transsubstantive privacy provision. Exemption 6 shields from public view "personnel and medical files and similar files" for which disclosure "would constitute a clearly unwarranted invasion of personal privacy."[63] Under this provision, agencies must weigh the public interest in disclosure against the individual's interest in keeping the requested records private.[64]

Several states have followed suit. Roughly half of the states have enacted a general privacy exemption that either replicates or closely tracks the language of the federal privacy provision.[65] And many state courts have adopted the federal courts' balancing test as their own.[66] In this way, federal and state privacy protections have converged over time.

The other half of the states have not adopted a broad, transsubstantive privacy shield. Yet they still protect private information in other ways—for example, through the common law or through state constitutional provisions.[67] Virtually

[60] *Id.* at 503-05 (finding and discussing law enforcement's substantial role in shaping federal privacy laws on a variety of subjects).

[61] *Id.* at 506 (describing statutory exceptions permitting law enforcement to access emails and health records).

[62] There are also subject-specific privacy laws that govern government records. *See, e.g.*, Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721(b) (governing driver's license records); Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (1976) (codified as amended in scattered sections of 26 U.S.C.) (governing tax filer information); Privacy Act of 1974, 5 U.S.C. § 552a.

[63] 5 U.S.C. § 552b(c)(6).

[64] *Id.*; *see also* Dep't of Air Force v. Rose, 425 U.S. 352, 372 (1976).

[65] *See* State Law Comparisons Spreadsheet, *supra* note 44.

[66] *See, e.g.*, Stilley v. McBride, 965 S.W.2d 125, 127 (1998); Seelig v. Sielaff, 201 A.D.2d 298, 299 (N.Y. App. Div. 1994) (adopting federal balancing standard for New York FOIA equivalent). *But see, e.g.*, ACLU Found. of Iowa, Inc. v. Recs. Custodian, Atl. Cmty. Sch. Dist., 818 N.W.2d 231, 233-34 (Iowa 2012) (declining to apply FOIA Exemption 6 precedent to state law privacy exemption).

[67] *See* State Law Comparisons Spreadsheet, *supra* note 44.

every public records law also contains a set of narrower and more targeted privacy exemptions.[68] In many states, private information is largely shielded through dozens or even hundreds of these one-off, subject-specific privacy carveouts.[69]

In addition to these transsubstantive privacy shields, many public records laws contain separate privacy exemptions specifically for law enforcement agencies. At the federal level, Exemption 7(C) of FOIA protects the records of law enforcement agencies when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[70] As a result, there are two different standards for government privacy claims: Exemption 6 binds all agencies,[71] but Exemption 7(C) binds only law enforcement.[72] And this law-enforcement-specific exemption requires a lesser showing of potential privacy harm to keep information secret. In short, it is easier for federal law enforcement agencies to withhold records on privacy grounds than it is for all other federal agencies.[73]

Once again, some states have adopted the federal model. At least seven state legislatures have enacted a law enforcement privacy exemption that either imitates or closely tracks the language of FOIA's Exemption 7(C).[74] Five other states have enacted separate police-specific privacy exemptions in ways that depart from the federal example.[75]

That leaves most states without a police-specific privacy provision. But that doesn't mean law enforcement records in these places lack protection. Rather, many states have enacted generalized privacy exemptions. And most state statutory codes contain narrower and more targeted privacy carveouts as well. These latter protections generally take one of two forms: provisions that protect the privacy of citizens; and provisions that protect the privacy of police officers.

---

[68] *Id.*

[69] *See* discussion *infra* Sections I.B-C.

[70] 5 U.S.C. § 552(b)(7)(C).

[71] *Id.* § 552(b)(6).

[72] *Id.* § 552(b)(7)(C).

[73] *Compare id.* § 552b(6) (requiring that agencies show disclosure "would constitute a clearly unwarranted" invasion of privacy"), *with id.* § 552(b)(7)(C) (requiring that disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy"). *See also* U.S. DOJ, GUIDE TO THE FREEDOM OF INFORMATION ACT: EXEMPTION 7, at 10 n.26 (2024), https://www.justice.gov/oip/media/1379251/dl [https://perma.cc/3XU9-6TLY] (providing that non-law-enforcement agencies may invoke Exemption 7 if engaged in certain types of investigations).

[74] ALASKA STAT. § 40.25.120(a)(6)(C) (2025); IDAHO CODE § 74-124(1)(c) (2025); MD. CODE ANN., GEN. PROVIS. § 4-351(b)(3) (LexisNexis 2024); MICH. COMP. LAWS ANN. § 15.243(b)(iii) (West 2025); S.C. CODE ANN. § 30-4-40(a)(3)(C) (West 2025); VT. STAT. ANN. tit. 1, § 317(c)(5)(A)(iii) (2025).

[75] *See* State Law Comparisons Spreadsheet, *supra* note 44.

B. *Citizen Privacy Protections*

Law enforcement agencies at all levels gather vast amounts of information about the public.[76] The transparency law regime reflects this reality. Public records laws contain scores of provisions shielding police-gathered data about citizens from public view. Such protections are not always justified exclusively on privacy grounds: There may be safety or anticircumvention concerns motivating them as well.[77] But privacy concerns operate as a central reason for withholding these various categories of records.

Protections for criminal justice records are especially common. These include sealing statutes, which are provisions that automatically seal criminal justice records. Examples include statutes sealing the records of juvenile offenders,[78] as well as the records of individuals accused but not convicted of a crime.[79] They also include provisions shielding more specific categories of criminal justice records, such as mug shot photos,[80] arrest records,[81] or the records of incarcerated individuals.[82]

[76] *See infra* Section II.B.2.

[77] For example, protections for witnesses, victims, and confidential informants are often justified on both privacy and anticircumvention grounds. *See, e.g.*, 5 ILL. COMP. STAT. ANN. 140/7(1)(d)(iv) (West 2024) (shielding identity of all witnesses, including victims, "when disclosure would interfere with an active criminal investigation"); VT. STAT. ANN. tit. 1, § 317(c)(5)(D) (2025) (shielding "the identity of a private individual who is a witness to or victim of a crime").

[78] *See* Joy Radice, *The Juvenile Record Myth*, 106 GEO. L.J. 365, 407 (2018) ("[E]very state has an extinguishing statute on the books to expunge, seal, or set-aside juvenile records.").

[79] *See, e.g.*, N.Y. CRIM. PROC. LAW § 160.50 (McKinney 2025) (automatically sealing criminal proceedings that end in favor of the accused).

[80] *See, e.g.*, GA. CODE ANN. §§ 35-1-19(c)-(d), 50-18-72(a)(4) (2024) (imposing procedures designed to prevent release of mug shots to websites that require fee for their deletion); HAW. REV. STAT. ANN. §§ 92F-13(4), 831-3.2 (LexisNexis 2024) (prohibiting disclosure of mug shots of people whose records have been expunged); OR. REV. STAT. ANN. § 163A.225 (West 2024) (exempting pictures of juvenile offenders from disclosure); Cowles Publ'g Co. v. Spokane Police Dep't, 987 P.2d 620, 624 (Wash. 1999) (citing WASH. REV. CODE ANN. § 70.48.100(2) (West 2024)) (exempting mug shots from disclosure under state statute).

[81] *See, e.g.*, LA. STAT. ANN. § 44:3(A)(4)(a) (2024) (exempting arrest records "until a final judgment of conviction or the acceptance of a plea of guilty"); ME. STAT. tit. 16, § 703(2) (2025) (restricting disclosure to one year after arrest if no criminal prosecution has been pursued).

[82] *See, e.g.*, ARK. CODE ANN. § 12-27-113(e)(1)-(2) (2025) (exempting inmate records created by Department of Corrections); KAN. STAT. ANN. 45-221(a)(29) (West 2025) (exempting correctional records pertaining to specific inmate from disclosure); LA. STAT. ANN. § 15:574.12(A) (2024) (exempting records gathered by parole boards); VA. CODE ANN. § 2.2-3706(B)(4) (2024) (providing that inmate records are subject to discretionary release by agency).

Civilian privacy exemptions also include protections for other individuals caught up in the justice system, including victims,[83] witnesses,[84] informants,[85] and jurors.[86] Such protections are often explicit. But they may also be embedded within shields for adjacent categories of police records—for example, 911 calls, which have the secondary effect of protecting private information about crime victims and witnesses.[87]

Another group of exemptions shield data collected by specific surveillance technologies or systems, such as automated license plate records[88] or biometric data.[89] They also include protections for aggregated police information. Some states have enacted explicit protections for data and records housed in Fusion Centers, for example, which are federal-state information sharing centers established in the wake of September 11.[90] Still others shield specific police databases like gun permit applications.[91]

[83] *See, e.g.*, 65 PA. CONS. STAT. § 67.708(b)(16)(v) (2025). Virtually every state exempts victim information from disclosure under its public records law. *See 7. Victims*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/open-government-sections/7-victims/ [https://perma.cc/Q8T8-GGH5] (last visited Apr. 10, 2025) (surveying relevant statutes and case law in each state and the District of Columbia).

[84] *See, e.g.*, N.C. GEN. STAT. § 132-1.4(d) (2025) (permitting the withholding of "complaining witness" names under certain conditions); VT. STAT. ANN. tit. 1, § 317(c)(5)(D) (2025) (withholding identity of most crime victims).

[85] Nearly all states exempt information about confidential informants from public disclosure. *See 9. Confidential Informants*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/open-government-sections/9-confidential-informants/ [https://perma.cc/73KV-DTE4] (last visited Apr. 10, 2025) (surveying relevant statutes and case law in each state and the District of Columbia).

[86] *See, e.g.*, ALA. CODE § 12-16-70 (2025) (excluding juror lists from disclosure).

[87] *See, e.g.*, GA. CODE ANN. § 50-18-72(a)(26) (2025) (providing for the redaction of some information in 911 call tapes); MISS. CODE ANN. § 19-5-319(2) (2025) (prohibiting disclosure of most 911 calls without court order or subpoena); MO. ANN. STAT. § 610.150 (West 2024) (exempting records relating to 911 calls); Hill v. E. Baton Rouge Par. Dep't of Emergency Med. Servs., 2005-1236, p. 5 (La. App. 1 Cir. 12/22/05), 925 So. 2d 17, 21 (holding that 911 call recordings are protected under the state's privacy exemption).

[88] *See, e.g.*, GA. CODE ANN. § 35-1-22(f) (2025); UTAH CODE ANN. § 63G-2-305(63) (LexisNexis 2024).

[89] *See, e.g.*, FLA. STAT. ANN. § 119.071(5)(g) (West 2024); WASH. REV. CODE ANN. § 40.26.020(5) (West 2024).

[90] *See, e.g.*, KAN. STAT. ANN. § 48-3709 (West 2025); LA. STAT. ANN. § 44:4.1(D) (2024); NEV. REV. STAT. ANN. § 239C.210 (LexisNexis 2025); VA. CODE ANN. § 52-48(A) (2024); W. VA. CODE ANN. § 15A-12-5 (LexisNexis 2025).

[91] *See, e.g.*, ALA. CODE § 13A-11-75(k) (2025) (shielding information on gun permits from public disclosure, except aggregate or anonymized data); ALASKA STAT. § 18.65.770 (2025); ARIZ. REV. STAT. ANN. § 13-3112(J) (2025); ARK. CODE ANN. § 25-19-105(b)(18) (2025); CONN. GEN. STAT. ANN. § 29-28(d) (West 2025); DEL. CODE ANN. tit. 29, § 10002(o)(11) (2025). For a full list of such statutes, see Koningisor, *supra* note 19, at 645 n.177.

An important subset of these technology-specific provisions protects body-worn camera videos from public disclosure. State and local governments have taken different approaches to this issue. At the state level, roughly 40% of legislatures have enacted a specific statute governing the release of body camera footage.[92] But these provisions vary. Some exclude all body camera footage from public view.[93] Others require disclosure to the individuals depicted in the videos, or to their families.[94] Still others dictate specific categories of videos that must be disclosed—for instance, those that show the use or attempted use of deadly force by police.[95]

Many of these provisions bake privacy considerations into the text of the law.[96] Some shield body camera footage when it is taken inside a private residence or healthcare facility,[97] for example, or when it depicts a victim of sexual or domestic abuse.[98] Others prohibit disclosure of portions of a video

[92] *See* Body Camera Provisions Spreadsheet (on file with author).

[93] *See, e.g.*, S.C. CODE ANN. § 23-1-240(G)(1) (West 2025). Individual agencies are also empowered to develop their own body camera rules about disclosure. *See id.* § 23-1-240(B); *see also* TEX. CODE CRIM. PROC. ANN. art. 2B.0112(c)-(d) (West 2023) (excluding all body camera footage from public records disclosure unless it is used in criminal investigation).

[94] *See, e.g.*, COLO. REV. STAT. § 24-31-902(2) (2025); FLA. STAT. ANN. § 119.071(2)(l)(4) (West 2024); LA. STAT. ANN. § 44:3(K)(1) (2024); MINN. STAT. ANN. § 13.825 subd. 2(b) (West 2025); N.C. GEN. STAT § 132-1.4A(c) (2025); *see also* KY. REV. STAT. ANN. § 61.168(5)(d) (West 2025) (providing that individual captured in body camera footage may be permitted to view recording but not to obtain copy of it); OHIO REV. CODE ANN. § 149.43(17)(b) (LexisNexis 2025) (restricting disclosure without family's consent of video depicting someone's death). Other statutes address conditions under which body camera recordings are required. *See, e.g.*, N.J. STAT. ANN. § 40A:14-118.3 (West 2025) (requiring officers to record "audio and video while acting in the performance of the officer's official duties" and providing exceptions).

[95] *See, e.g.*, CAL. GOV'T CODE § 7923.625 (West 2025) (providing for disclosure of body camera footage in serious incidents); ME. STAT. tit. 16, § 806-A (2025) (providing that Attorney General must weigh public interest in disclosure of video depicting use of deadly force by police against harms); MINN. STAT. ANN. § 13.825 subd. 2(a)(1) (West 2025) (making public "the use of force by a peace officer that results in substantial bodily harm").

[96] *See, e.g.*, LA. STAT. ANN. § 44:3(A)(8) (2024) (exempting body-worn camera footage "found by the custodian to violate an individual's reasonable expectation of privacy"); WASH. REV. CODE ANN. § 42.56.240(14) (West 2024) (exempting body-worn camera recordings "to the extent nondisclosure is essential for the protection of any person's right to privacy").

[97] For examples of private residence provisions, see FLA. STAT. ANN. § 119.071(2)(l)(2)(a) (West 2024); OHIO REV. CODE ANN. § 149.43(17)(p) (LexisNexis 2025) (exempting recordings of "[t]he interior of a residence" from definition of public record); NEV. REV. STAT. ANN. § 289.830(1)(d)(1) (LexisNexis 2025); N.H. REV. STAT. § 105-D:2(IX) (2025); and N.D. CENT. CODE § 44-04-18.7(9) (2025). For an example of a healthcare facility provision, see KY. REV. STAT. ANN. § 61.168(4)(b) (West 2025). *See also* OHIO REV. CODE ANN. § 149.43(17)(i) (LexisNexis 2024).

[98] *See, e.g.*, CONN. GEN. STAT. ANN. § 29-6D(g)(2)(B) (West 2025); IND. CODE ANN. § 5-14-3-5.2(e)(1)(B)(vii) (West 2025).

when it contains depictions of a minor.[99] One state requires the blurring of all faces that appear in the video, including the faces of on-duty officers, before a video may be released.[100]

Finally, there is a subset of privacy provisions that implicate law enforcement records in less obvious ways. For instance, many states extend protections for autopsy reports, which may shed light on the adequacy of a law enforcement investigation,[101] or for motor vehicle accident reports, which are often held by the police.[102] Countless other exemptions implicate privacy interests even if they are not always framed as such. Thousands of such statutory provisions are scattered across the federal and state codes, offering protection for medical records, tax records, bank records, military records, and more.[103] These exemptions, too, can be used by police to shield law enforcement activities when qualifying documents end up in police files.

C. *Police Officer Privacy Protections*

A final set of privacy protections are granted to law enforcement personnel specifically. Law enforcement officers enjoy access to privacy protections that are not available to other government actors or to the public at large. Some of these protections are more limited—for example, some states shield personal identifying information about a police officer from disclosure to any

[99] *See, e.g.*, OKLA. STAT. ANN. tit. 51, § 24A.8(A)(9)(c) (West 2024).

[100] OR. REV. STAT. ANN. § 192.345(A)(40)(c) (West 2024) ("A video recording disclosed under this subsection must, prior to disclosure, be edited in a manner as to render the faces of all persons within the recording unidentifiable."). In the remaining states—those without explicit body camera provisions—access to body camera videos is resolved through other statutory provisions, such as investigatory provisions. *See, e.g.*, ALASKA STAT. § 40.25.120(A)(6)(c) (2025) (permitting police to withhold records on privacy grounds); GA. CODE ANN. § 50-18-72(a)(4) (2025) (shielding records that would interfere with ongoing law enforcement investigation).

[101] *See, e.g.*, ALASKA STAT. § 12.65.020(b) (2025); ARK. CODE ANN. § 14-15-304(a)(1) (2025); IND. CODE ANN. § 5-14-3-4(a)(11) (West 2025) (exempting autopsy-related documents as public records that may not be disclosed by public agencies unless access is specifically required by statute, court order, or rules of evidence). Some states combine the position of sheriff and coroner. *See* Hillel Aron, *Push on to Separate Coroners from Law Enforcement in California*, COURTHOUSE NEWS SERV. (Jan. 6, 2022), https://www.courthousenews.com/push-on-to-separate-coroners-from-law-enforcement-in-california/.

[102] *See, e.g.*, LA. STAT. ANN. § 32:398(H)(1) (2024).

[103] Such exemptions are too numerous to cite. For an example of the myriad exemptions that implicate privacy concerns, see, e.g., TENN. COMPTROLLER OF THE TREASURY, STATUTORY EXCEPTIONS TO THE TENNESSEE PUBLIC RECORDS ACT (2018), https://comptroller.tn.gov/content/dam/cot/orc/documents/oorc/2018-01-19_ExceptionstotheTennesseePublicRecordsActFinal.pdf [https://perma.cc/4BWB-CLF5].

incarcerated individual.[104] Others protect against disclosure of any private information about a police officer to any member of the public.[105] Such protections are justified on both safety and privacy grounds.[106]

A more contested set of exemptions shield the personnel files of law enforcement officials. Whether the public should be able to access police disciplinary material, and under what conditions, has been the subject of intense debate. Several states have enacted legislation rolling back protections for these types of materials in recent years.[107] Even so, gaining access to police disciplinary records remains difficult across the country.[108]

Once again, states take different approaches. Some make all government personnel files confidential.[109] Many apply a balancing test that weighs the public interest in disclosure against the private interest in secrecy.[110] But even in the states with more favorable disclosure regimes, broad categories of

[104] *See, e.g.*, IND. CODE ANN. § 5-14-3-4(23) (West 2025) (exempting from public records any records requested by an offender or their agent that contain personal information relating to a correctional officer, probation officer, law enforcement officer, or their families, among others).

[105] MISS. CODE ANN. § 25-61-12(1) (2025); *see also* MICH. COMP. LAWS ANN. § 15.243(1)(s) (West 2025).

[106] *See, e.g.*, Stilley v. McBride, 965 S.W.2d 125, 128 (Ark. 1998) (relying on both privacy and safety concerns to withhold home addresses of police officers).

[107] For a list of some of these proposed laws, see *Police Legislation Database*, NCSL, https://www.ncsl.org/civil-and-criminal-justice/policing-legislation-database (last updated Apr. 9, 2024).

[108] It is difficult to quantify the number of states that provide meaningful access to police disciplinary records. Very few states wholly restrict or release these records. The vast majority make some categories of police personnel records public while withholding others—for example, some states will disclose only substantiated complaints or only allegations of serious misconduct. *See* Kallie Cox & William Freivogel, *Police Misconduct Records Secret, Difficult to Access*, PULITZER CTR. (Jan. 24, 2022), https://pulitzercenter.org/stories/police-misconduct-records-secret-difficult-access.

[109] *See, e.g.*, ALASKA STAT. § 39.25.080(a) (2025) (holding state personnel records confidential and not open to public inspection unless otherwise exempted); DEL. CODE ANN. tit. 11, § 9200(c)(12) (2025) (classifying records of police investigations or disciplinary grievances as confidential); IDAHO CODE § 74-106(1) (2025) (exempting from disclosure all personnel records of current or former public officials other than compensation); KAN. STAT. ANN. § 45-221(a)(4) (West 2024); 65 PA. STAT. AND CONS. STAT. ANN. § 67.708(b)(7) (West 2025); S.D. CODIFIED LAWS § 1-27-1.5(7) (2025); VA. CODE ANN. § 2.2-3705.1(1) (2024).

[110] *See, e.g.*, Fraternal Ord. of Police, Metro. Police Lab. Comm. v. District of Columbia, 124 A.3d 69, 79 (D.C. 2015) (applying balancing test to personnel records); Peer News LLC v. City & Cnty. of Honolulu, 376 P.3d 1, 10 (Haw. 2016); Hagen v. Bd. of Regents of Univ. of Wis. Sys., 2018 WI App 43, ¶ 5, 383 Wis. 2d 567, 571-72, 916 N.W.2d 198, 200 (Wis. Ct. App. 2018) (same).

disciplinary records—for example, unsubstantiated complaints against police officers—often remain shielded from public view.[111]

II. COOPTING PRIVACY

Law enforcement agencies gather vast amounts of sensitive information about the public. They have always done so through day-to-day interactions with citizens. But police now enjoy expanded powers of surveillance,[112] as well as access to volumes of data generated both externally by private companies and internally by the nation's system of mass incarceration.[113] The legislative response has been to grant police ever-stronger secrecy protections to shield this amassed civilian data from public view.[114] This comes with an interlocking set of privacy-accountability trade-offs. It also comes with an increased risk of abuse. Law enforcement agencies invoke these privacy protections as a pretext to shield their own activities from public scrutiny.

This Part catalogues different types of police cooption of privacy interests. It borrows privacy law scholar Neil Richards's approach to privacy cooption, which he defines as "the co-option of privacy rules to serve institutional rather than individual interests."[115] This definition is broad enough to reach an array of examples. It encompasses police privacy claims that (1) involve few or no cognizable privacy interests, (2) involve substantially overstated privacy

[111] For example, few states provide public access to unsubstantiated complaints. *See* Cox & Freivogel, *supra* note 108.

[112] *See, e.g.*, 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, 24-27 (2023) (describing privacy harms imposed by police surveillance); Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1, 1 (2013) (describing rapid rise in police technological surveillance).

[113] *See* Sarah Brayne, *Dye in the Cracks: The Limits of Legal Frameworks Governing Police Use of Big Data*, 65 ST. LOUIS U. L.J. 823, 825 (2021) (noting one-third of U.S. adults have records with criminal justice agencies); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1955-56 (2013) (describing police acquisition and compulsion of private-sector-generated data).

[114] *See supra* Part I.

[115] Richards, *supra* note 28, at 1514. Richards was primarily concerned with corporate privacy cooption, but the definition is applicable to the government context as well. *Id.* Scholars have proposed alternative definitions of legal cooption as well. *See, e.g.*, Banteka, *supra* note 28, at 1884 (defining "legal pretext" in context of policing as "when the government justifies an action with an explanation that is not the true reason motivating police activity, but is legally sufficient to justify that action"). Further, this Article does discuss individual officers' reliance on privacy protections as a form of privacy cooption, given that these examples still fit the definition so long as the arguments are being made to advance law enforcement agencies' institutional interests and needs (such as shielding the department from political and public fallout for the abusive actions taken by individual officers). *See* discussion *infra* Section II(C).

interests, or (3) selectively invoke privacy protections to advance the institutional interests of police.

It also takes an expansive view of the concept of privacy. While this is a contested issue,[116] this Part assumes that any personally identifiable information contained in government records may implicate privacy concerns.[117] It also assumes that there is a sliding scale of privacy interests, one in which especially sensitive information—for example, medical information—will involve more significant privacy interests than bureaucratic or administrative information, such as an employee's ID number.[118] Yet privacy is subjective,[119] as well as context-specific.[120] The severity of any particular privacy intrusion will depend in part on the specifics of that incident.

A. *Police Records Data*

There are two central obstacles to studying privacy claims by police. The first is that it is difficult to identify the motives behind any single agency decision or legislative action. There are often multiple decisionmakers involved. And examining the pretextual use of privacy protections requires peeking behind the curtains of the decision-making process to determine what actually drives the government to withhold information. Government actors will occasionally admit that privacy concerns have been invoked as a pretext to advance some other interest or goal. But this almost exclusively occurs behind closed doors, with the admission becoming public only after the incident comes under scrutiny. The Daniel Prude case offers an example of this.[121]

Furthermore, such explicit admissions are rare. More often, the pretextual use of privacy shields leaves the true use to be inferred from context. This task

---

[116] Courts and scholars have long debated what types of information and activities should be encompassed under the umbrella of "privacy." For two opposing perspectives on this issue, *compare* Solove, *supra* note 35, at 481-82 (proposing taxonomy of "activities that pose privacy problems"), *with* María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507, 552-54 (2024) (proposing functionalist definition of "privacy problems").

[117] *See* U.S. DOJ v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) ("[P]rivacy encompass[es] the individual's control of information concerning his or her person."). For a discussion of the problem of inferences, see *infra* notes 252-253 and accompanying text.

[118] Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1131 (2015).

[119] *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing subjective dimension of privacy interests in Fourth Amendment context).

[120] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2010) ("[F]inely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g., education, health care, and politics).").

[121] CELLI ET AL., *supra* note 3, at 9-10 (detailing police's use of ostensible HIPAA concerns to prevent disclosure of incendiary arrest video).

becomes more complicated when mixed motives are involved.[122] A public records denial may be driven by anti-accountability goals but still advance some genuine privacy interests. This adds to the difficulty of identifying and describing specific instances of privacy cooption.

As a result, the case for privacy cooption is often circumstantial.[123] Contextual clues, such as discrepancies between the government's stated justifications and the actual substance of the underlying records, may serve as evidence of pretextual motives.[124] The government's privacy argument may also be so strained that it serves as a plausible example of privacy cooption on its own terms. And the government's inconsistent treatment of information deemed private may serve as further evidence. Yet any single police assertion may be open to multiple interpretations, and it remains difficult to make conclusive assessments of motive in this context. I have tried to address this ambiguity by stating up front what is known versus what must be inferred about the government's motives and intent.[125]

The second major obstacle to studying police privacy claims is that there is limited public records data available at the state and local levels. The federal government maintains detailed information about FOIA requests, and this data reveals that federal law enforcement agencies rely extensively on privacy exemptions. In 2023, for example, the FBI invoked a privacy exemption in at least a quarter of the roughly 19,000 requests that it processed.[126] The Bureau of Alcohol, Tobacco, Firearms and Explosives withheld records on privacy

[122] For discussion of mixed motives in the context of privacy pretexts, see Van Loo, *Privacy Pretexts*, *supra* note 28, at 111. For a discussion of the complexities of mixed motives in the law more broadly, see Andrew Verstein, *The Jurisprudence of Mixed Motives*, 127 YALE L.J. 1106, 1114 (2018).

[123] *Cf.* Van Loo, *Privacy Pretexts*, *supra* note 28, at 11 ("Because determining corporate motive is notoriously difficult, the case for a privacy pretext is usually circumstantial.").

[124] *See id.*

[125] A further critique might be: Why do law enforcement motives matter? If the privacy interests in a government record are sufficiently strong, withholding it will be the correct result, regardless of the motivations of the agency. The response, I think, is that there is an inherent accountability and democratic oversight cost to any government withholding on privacy grounds. And to properly assess these two competing interests—privacy on the one hand, and democratic oversight on the other—we must try to understand the nature of that accountability loss. Such information is a relevant input when weighing privacy benefits against governance harms, regardless of the output.

[126] The FBI processed 19,359 requests total. U.S. DOJ, UNITED STATES DEPARTMENT OF JUSTICE ANNUAL FREEDOM OF INFORMATION ACT REPORT: FISCAL YEAR 2023, at 22 (2023), https://www.justice.gov/oip/media/1339106/dl [https://perma.cc/CDM7-8RXN]. It invoked Exemption 6 in 4,993 requests and Exemption 7(C) in 5,015 requests. *Id.* at 26. However, because the data doesn't specify whether there are any overlaps between these requests, it is impossible to calculate the percentage of total requests in which a privacy exemption was invoked. 25.9% represents the lowest possible percentage of responses invoking a privacy exemption—it assumes that all Exemption 7(C) responses also included an Exemption 6 response. The true percentage is likely higher.

grounds in at least 22% of the requests it received that same year.[127] And the Drug Enforcement Administration invoked privacy protections in roughly a third of the total requests that it processed.[128]

It is more difficult to study agency denials at the subfederal level. There are roughly 18,000 law enforcement agencies in this country, the vast majority of which are state and local entities.[129] No state compiles comprehensive public records data.[130] Furthermore, when individual state and local agencies do compile records data, they almost never track the statutory exemptions used.[131] Anecdotal evidence suggests certain police departments rely heavily on privacy exemptions.[132] Yet these sources of data are limited, and such findings are not necessarily generalizable.[133] As a result, it becomes difficult to determine how

[127] *Id.* at 22, 26 (568 Exemption 6 and 399 Exemption 7(C) responses out of 1,774 total requests).

[128] *Id.* at 22, 26 (514 Exemption 6 and 532 Exemption 7(C) out of 1,646 requests).

[129] U.S. DOJ, NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 1 (2016), https://bjs.ojp.gov/content/pub/pdf/nsleed.pdf [https://perma.cc/3427-JJJH].

[130] Only a handful of states track statewide agency requester data, and no state tracks public records requests at the local level. *See* Christina Koningisor, *Transparency Deserts*, 114 NW. U. L. REV. 1461, 1480 (2020) (describing these laws).

[131] *Id.*

[132] A handful of private websites make requesting information public, including MuckRock, which allows requesters to streamline the process and file their requests publicly. MUCKROCK, https://www.muckrock.com/ [https://perma.cc/2P7Z-RBH5] (last visited Apr. 10, 2025). I reviewed roughly 1,000 of these requests processed by the New York City Police Department and the Chicago Police Department between 2011 and 2023. The New York City Police Department ("NYPD") invoked privacy exemptions in 23% of the MuckRock requests that it processed. NYPD MuckRock Data (on file with author) (privacy exemptions cited in 128 out of 556 processed requests). The Chicago Police Department ("CPD") invoked privacy exemptions in 38% of responses processed through MuckRock. CPD MuckRock Data (on file with author) (privacy exemptions cited in 198 out of 528 processed requests).

[133] The MuckRock data, discussed *supra* note 132, represents only a fraction of requests submitted to these two agencies across these time periods. Further, public records trends of two large urban agencies are not necessarily representative of trends in other police departments. *See* Maria Ponomarenko, *The Small Agency Problem in American Policing*, 99 N.Y.U. L. REV. 202, 205 (2024) ("The vast majority of police departments . . . look nothing like the sprawling bureaucracies that police the urban core."). This data is also unrepresentative in terms of the population of requesters who use MuckRock rather than submitting requests directly through an agency portal. *Compare* Koningisor, *supra* note 19, at 634 (finding that roughly 85% of MuckRock requesters are academics, non-profit employees, or journalists), *with* COAL. OF JOURNALISTS FOR OPEN GOV'T, FREQUENT FILERS: BUSINESSES MAKE FOIA THEIR BUSINESS 1 (2006), https://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/intl/businesses_make_foia_their_business.pdf [https://perma.cc/HQW4-N2AC] (reporting FOIA analytics revealing "more than 60 percent of the requests came from commercial interests").

often privacy exemptions are invoked, and nearly impossible to quantify how often privacy protections are being coopted to serve other ends.[134]

With these caveats in mind, this Part explores different examples of privacy cooption by police. It first examines police cooption of citizen privacy shields as a mechanism for evading public scrutiny. It then explores the problem of cooption in the context of law enforcement officers' own privacy claims—or the ways that police use their own privacy interests as a shield against broader public oversight.

B. *Citizen Privacy as Police Secrecy*

Law enforcement agencies routinely invoke the privacy interests of the public as a reason to keep police records and information secret. This takes different forms. First, law enforcement agencies invoke the privacy interests of specific categories of individuals involved in the criminal justice system—witnesses, victims, informants, jurors, the accused, and so on—as a reason for nondisclosure. Second, police invoke the public's privacy interests to withhold records relating to police surveillance of the public at large, often conducted via mass surveillance technologies like facial recognition technologies, automated license plate readers, gunshot detection software, cell site simulator devices, and more. These two categories of citizen-focused privacy shields are explored below.

1. Privacy Protections for Criminal Justice Records

Public records laws contain myriad privacy protections for specific categories of criminal justice records, including those of crime victims, witnesses, juveniles accused or convicted of a crime, jurors, and more.[135] These protections can serve genuine privacy goals. They may make it easier for a formerly incarcerated person to start over, for example, or encourage crime victims or witnesses to come forward and report a crime.[136] Yet the text of these statutory protections is often broad and ambiguous. As a result, these privacy-focused protections become vulnerable to cooption. Police utilize these citizen privacy provisions to serve anti-accountability ends.

---

[134] As a result of the difficulty of obtaining empirical data around even baseline levels of privacy exemption use, this Part relies largely on anecdotal examples. Some involve acts of police violence that have garnered significant media attention. Others are pulled from cases. Yet only a fraction of public records denials ever makes it to court. The overwhelming majority of privacy denials at the administrative level are never litigated. *See* Koningisor, *supra* note 130, at 1478-79.

[135] *See supra* Section I.B.

[136] Steven Raphael, *Should Criminal History Records Be Universally Available?*, 5 CRIMINOLOGY & PUB. POL'Y 515, 517, 519 (2006); John Losinger, *Electronic Access to Court Records: Shifting the Privacy Burden Away from Witnesses and Victims*, 36 U. BALT. L. REV. 419, 441 (2007).

The most extreme example is when law enforcement agencies withhold records of police killings on the grounds that disclosure would violate the privacy interests of the deceased. Again, the Daniel Prude request offers an illustration. The police claimed that it could not release footage showing police misconduct because doing so would violate Prude's own privacy interests. It did so even against the objections of Prude's family, who wanted the video to be disclosed.[137]

It is difficult to determine how often this type of cooption occurs, given the limitations of the police records data. The government does not accurately track police use of force incidents nationwide.[138] It does not even record how many people are killed by the police each year.[139] Yet anecdotally, police agencies around the country have invoked the privacy interests of the victims of police violence in similar ways. A reporter from *ProPublica*, for example, filed records requests to obtain body camera footage of all police killings that occurred nationwide in a single month in 2022.[140] Of the twenty-three agencies that rejected his requests, seven cited the privacy interests of the victim.[141]

There are other examples as well.[142] New York City Police Department ("NYPD") officers shot and killed a man named Miguel Richards in his apartment in the Bronx in 2017. It was the first NYPD-caused death captured on

[137] *See* discussion *supra* notes 8-10 and accompanying text.

[138] The best data available comes not from the FBI but from media and activist organizations that track this data from outside the government. *See* Kimberly Kindy, Marc Fisher, Julie Tate & Jennifer Jenkins, *A Year of Reckoning: Police Fatally Shoot Nearly 1,000*, WASH. POST (Dec. 26, 2015), https://www.washingtonpost.com/sf/investigative/2015/12/26/a-year-of-reckoning-police-fatally-shoot-nearly-1000/.

[139] *Id.*

[140] Umar Farooq, *Body Cameras Were Sold as a Tool of Police Reform. Ten Years Later, Most of the Footage Is Kept from Public View*., PROPUBLICA (Dec. 18, 2023, 5:00 AM), https://www.propublica.org/article/body-camera-videos-police-killings-remain-hidden-from-public [https://perma.cc/R9YZ-JMHK].

[141] E-mail from Umar Farooq, Reporter, to author (Jan. 3, 2024) (on file with author). Six of these were from agencies in Texas. *Id.*

[142] *See, e.g.*, Jared Strong & Erin Jordan, *Privacy vs. the Public's Right to Know at Center of Debate over Police Video Recordings*, DES MOINES REG. (Apr. 25, 2021, 5:00 AM), https://www.desmoinesregister.com/story/news/2021/04/25/privacy-vs-public-records-iowa-whos-allowed-see-police-videos-body-camera-footage-laws/7264767002/ [https://perma.cc/UPR4-M5LT] (discussing Maquoketa police's refusal to release officer's body camera video of fatal incident involving stun gun, citing violation of victim's privacy rights, despite victim's family's desire for video to be made public, along with similar refusals from other police departments, such as Chicago Police Department); Jo C. Goode, *'Denials . . . Are Disingenuous': Family of Fall River Man Killed by Police Sues for Report*, HERALD NEWS, https://www.heraldnews.com/story/news/courts/2022/02/02/anthony-harden-fall-river-ma-shot-killed-police-sues-bristol-county-da-police-reform-justice/9315331002/ [https://perma.cc/HQ74-CBA2] (last updated Feb. 3, 2022, 11:18 AM).

video by a police body-worn camera.[143] Yet the agency refused to release the footage to the public on the grounds that "disclosure would constitute an unwarranted invasion of Mr. Richards' and his family's personal privacy."[144] It did so even though the requester submitted affidavits from the Richards family stating that the family wanted the video to be made public.[145]

Similarly, the NYPD shot and killed a man named Kawaski Trawick in his home in April 2019. Again, the department cited the deceased man's own privacy interests as a reason to keep the video secret.[146] A judge later rejected this privacy claim as a "blanket denial" that the NYPD had asserted "in bad faith."[147]

Police have invoked the privacy interests of the relatives of the deceased as a reason for non-disclosure as well. For instance, in Uvalde, Texas, the city denied requests for records about the police's response to the mass shooting at an elementary school in 2022 on privacy grounds. It argued that the documents contained information about the "emotional/mental distress" of the shooting victims' relatives, and therefore the records about the police department's delayed response could not be disclosed.[148]

Law enforcement agencies also invoke the privacy interests of those who have filed misconduct or abuse claims against police officers. For example, New York state law automatically seals all records relating to a criminal action that terminates in favor of the accused.[149] Police misconduct claims often arise out of a violent arrest. But if the person arrested is later released without charges, police agencies in New York can rely on this automatic sealing provision to prevent the release of body camera footage documenting the alleged police

[143] Eric Umansky & Umar Farooq, *How Police Have Undermined the Promise of Body Cameras*, PROPUBLICA (Dec. 14, 2023, 5:00 AM), https://www.propublica.org/article/how-police-undermined-promise-body-cameras [https://perma.cc/QQ7K-9FCU].

[144] N.Y. Laws. for the Pub. Int. v. N.Y.C. Police Dep't, 103 N.Y.S.3d 275, 278 (N.Y. Sup. Ct. 2019).

[145] Umansky, *supra* note 143.

[146] Article 78 Petition, New York Laws. for the Pub. Int. vs. N.Y.C. Police Dep't, No. 33 (N.Y. Sup. Ct. June 6, 2020), https://iapps.courts.state.ny.us/fbem/DocumentDisplayServlet?documentId=y5bNphwwLQSfGtYqL2uZ1A==&system=prod. The agency also invoked investigatory exemptions. *Id.*

[147] Transcript of Hearing at 14, 17, *New York Laws. for the Pub. Int.*, Doc. No. 70 (Nov. 5, 2021), https://s3.documentcloud.org/documents/21115911/fees-transcript.pdf [https://perma.cc/3EQZ-PRUG]. For a summary of the case and these proceedings, see Eric Umansky, *Judge Says NYPD Illegally Withheld Footage in Police Shootings*, PROPUBLICA (Nov. 23, 2021, 1:15 PM), https://www.propublica.org/article/judge-says-nypd-illegally-withheld-footage-in-police-shootings [https://perma.cc/W2JD-MZJZ].

[148] Letter from Cynthia Trevino, Att'y for the City of Uvalde, to Ken Paxton, Tex. Att'y Gen. 3 (June 16, 2022), https://s3.documentcloud.org/documents/22062880/uv_22-001_to_uv_22-148_-_ag_002_15_day_brief_4867-6084-58618_onjsm2l.pdf [https://perma.cc/US7V-68Q2].

[149] N.Y. CRIM. PROC. LAW § 160.50 (McKinney 2025).

misconduct.[150] The agency can argue that the privacy interests of the victim prevent the department from turning over evidence that would substantiate the victim's claims of police misconduct.

Evidence of the pretextual nature of such claims can be seen in how such agencies actually handle such footage. For instance, the NYPD has routinely cited citizen privacy interests as the reason it cannot disclose body camera footage to city investigators who are investigating the claims of police abuse.[151] Yet in these very same investigations, the department has shared the footage with the officers under investigation.[152]

Police commonly invoke laws protecting the privacy of minors as well, including minors who are accused or convicted of crimes, as well as those involved as bystanders, witnesses, or victims.[153] In 2019, for example, NYPD officers assaulted a man, breaking his foot and causing a brain bleed that left him hospitalized for nearly a week.[154] Seven body cameras worn by police officers captured the incident.[155] But the NYPD withheld all of the footage from the city's own police oversight board on the grounds that disclosure would violate the privacy interests of a teenager captured in the background of the film.[156] Once again, it did so while simultaneously granting the police officers accused of the assault the right to view the footage prior to any disciplinary proceeding.[157]

---

[150] *See* Memorandum from Olas Carayannis, Dir. of Quality Assurance and Improvement to Members of the Civilian Complaint Rev. Bd. 3-4 (July 5, 2019), https://www.nyc.gov/assets/ccrb/downloads/pdf/about_pdf/board/20190710_boardmtg_BWC_memo.pdf [https://perma.cc/9DRK-5ABE] ("The NYPD currently has a blanket policy of denying all BWC requests that are in any way related to a sealed case pursuant to CPL §§ 160.50/160.55."); Eric Umansky & Mollie Simon, *The NYPD Is Withholding Evidence from Investigations into Police Abuse*, PROPUBLICA (Aug. 17, 2020, 5:00 AM), https://www.propublica.org/article/the-nypd-is-withholding-evidence-from-investigations-into-police-abuse [https://perma.cc/ZBA7-W6UQ].

[151] Memorandum from Olas Carayannis, *supra* note 150, at 3. The NYPD and CCRB recently adopted an agreement stipulating that the NYPD will turn over body camera footage within ninety days of a request from the civilian review board. *See* Eric Umansky, *NYPD Will Stop Withholding Body-Camera Footage of Police Shootings from Civilian Investigators*, PROPUBLICA (Dec. 19, 2023, 5:00 AM), https://www.propublica.org/article/nypd-release-body-camera-footage-civilian-investigators [https://perma.cc/S77G-7EHE].

[152] Memorandum from Olas Carayannis, *supra* note 150, at 2-3 (noting police have right to view their BWC footage prior to disciplinary proceeding).

[153] *See* Banteka, *supra* note 28, at 1901-04 (describing police cooption of juvenile privacy protections).

[154] *See* Civilian Complaint Review Board Case Summary, https://s3.documentcloud.org/documents/7034573/Case-Summary-from-New-York-s-Civilian-Complaint.pdf [https://perma.cc/P4NK-EL7P]; *see also* Umansky & Simon, *supra* note 150.

[155] Umansky & Simon, *supra* note 150.

[156] *Id.*

[157] *See* Memorandum from Olas Carayannis, *supra* note 150, at 3.

Moreover, even when there are significant privacy interests at stake, such informational protections still impose an accountability cost. Many states protect the criminal records of individuals who have been accused but not convicted of a crime, for example.[158] The privacy interests in these protections are similar to those extended to unsubstantiated allegations against police—such provisions ensure that someone cleared of a crime will not have their reputation tarnished by the accusation. Yet these provisions can also operate as barriers to oversight of more systemic wrongdoing in the criminal justice system.

In 2014, for instance, the Brooklyn District Attorney's Office established a Conviction Review Unit to examine past cases for wrongful convictions.[159] The unit then vacated dozens of convictions involving police and prosecutorial misconduct.[160] Each time it recommended overturning a conviction, the Conviction Review Unit authored a report detailing the government misconduct in the case.[161]

Yet because the conviction was overturned, all records related to the case were automatically sealed.[162] When a *New York Times* reporter later sued for access, the court declined to release the reports on privacy grounds.[163] It did so even though the reports cast doubt on the integrity of these initial convictions.[164] As a result of such broad privacy shields, information both about specific acts of government misconduct and about broader structural inequities within the criminal justice system remained hidden from public view.

---

[158] *See, e.g.*, N.Y. CRIM. PROC. LAW § 160.5 (McKinney 2025) (detailing procedures implemented to ensure sealing of various records related to accused individual).

[159] *See* Press Release, Brooklyn District Attorney Publishes Report That Analyzes and Presents the Findings of His Conviction Review Unit (July 9, 2020), http://www.brooklynda.org/2020/07/09/brooklyn-district-attorney-publishes-report-that-analyzes-and-presents-the-findings-of-his-conviction-review-unit [https://perma.cc/P8WK-BRE6].

[160] *In re* N.Y. Times Co. v. Dist. Att'y of Kings Cnty., 111 N.Y.S.3d 691, 693 (N.Y. App. Div. 2019). The author participated as a member of the legal team representing the *New York Times* in this case.

[161] DIST. ATT'Y KINGS CNTY., 426 YEARS: AN EXAMINATION OF 25 WRONGFUL CONVICTIONS IN BROOKLYN, NEW YORK 4 (2020), http://www.brooklynda.org/wp-content/uploads/2020/07/KCDA_CRUReport_v4r3-FINAL.pdf [https://perma.cc/3BR2-Y227].

[162] *In re N.Y. Times Co.*, 111 N.Y.S.3d at 694.

[163] *Id.* at 693. The records may be released if the wrongly convicted person signs a release form.

[164] The *Times* asserted that the convictions were already in the public record, and the reports would at least cast doubt on their validity. *Id.* at 696. The District Attorney, however, noted that "in many cases, the conclusions of the reports were not that the individuals were innocent, but that they did not receive a fair trial." *Id.* at 697.

2. Privacy Protections for Surveillance Data

Police departments across the country gather vast amounts of information about the public. They do so through advanced surveillance technologies like automated license plate readers, which capture and aggregate license plate information; cell-site simulators, which gather information from nearby cell phones by imitating a cell tower; biometric surveillance technologies, including facial recognition tools; gunshot detection software; drone surveillance; and more.[165]

They also do so by aggregating information collected by various law enforcement agencies at all levels. Sometimes this data is both collected and combined by government actors. For example, law enforcement Fusion Centers are cooperative information-sharing sites where federal, state, and local law enforcement agencies aggregate data that each agency has gathered.[166] Other times, private actors obtain police data from different agencies, aggregate it, and then sell access back to the police. For instance, LexisNexis provides a service to streamline the police reporting process. The company then aggregates hundreds of thousands of police reports and sells access to the database back to law enforcement agencies.[167]

Finally, police gather data by compelling private companies to hand over information. Law enforcement agencies have always turned to private actors for data. But the scale and scope of such information collection and aggregation today is unprecedented.[168] Large-scale government requests and formalized surveillance programs compel private companies like Microsoft, Google, and Facebook to hand over large volumes of information to law enforcement agencies.[169]

The privacy interests in this information are clear. Through these programmatic surveillance and data aggregation efforts, law enforcement

[165] *See Street Level Surveillance*, EFF, https://www.eff.org/issues/street-level-surveillance [https://perma.cc/J747-H3NT] (last visited Apr. 10, 2025).

[166] *Fusion Center Locations and Contact Information*, HOMELAND SEC., https://www.dhs.gov/fusion-center-locations-and-contact-information [https://perma.cc/A9HF-HF7H] (last visited Apr. 10, 2025).

[167] Koningisor, *supra* note 130, at 1502-03.

[168] *See, e.g.*, Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298-99 (2014) (outlining way in which government coerces private owners to assist in speech regulation and surveillance); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 105 (2018).

[169] *See generally* GLENN GREENWALD, NO PLACE TO HIDE (2014) (describing global mass surveillance network operated by National Security Agency and facilitated by large U.S. technology companies); Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

agencies have obtained intimate details about citizens' lives.[170] And the transparency law regime reflects this through a wealth of both generalized and specific privacy exemptions.[171] Yet these protections have become so numerous and so broad that law enforcement agencies can and do invoke them as a way to shield vast amounts of police activity—including information about how law enforcement agencies are surveilling the public in the first place.

Consider an example. In 2015, the ACLU submitted a public records request to the Los Angeles Police and Sheriff's Departments for records relating to the agencies' use of automated license plate readers.[172] The law enforcement agencies refused to provide these materials on privacy grounds, arguing that disclosure of these records would violate the privacy of those whose data was captured by this surveillance technology.[173]

The problem with this argument is not that there aren't valid privacy interests at stake. Clearly, there are. The problem is that protecting the privacy interests of each individual citizen captured by this surveillance technology prevents the public from understanding the system-wide effects of this police activity—what data is gathered, how long it is stored, and with whom it is shared. When the state supreme court took up the case, it put its finger on this central tension in the agency's position. "Although we acknowledge that revealing raw ALPR data would be helpful in determining the extent to which ALPR technology threatens privacy," the court wrote, "the act of revealing the data would itself jeopardize the privacy of everyone associated with a scanned plate."[174]

Ultimately, the court struck a balance, ordering disclosure of anonymized license plate reader data.[175] Yet the police departments' initial effort to withhold all records relating to license plate reader data—including deidentified data—suggests that privacy concerns were not the sole factor driving the agencies' initial response.

There are other such examples of citizen data protections being used to shield police from public scrutiny. Consider the release of body-worn cameras. Many initially hailed this technology as a powerful tool to rein in police violence.[176] Yet police departments have largely retained control over this footage. This allows them to disclose it when it benefits police—when it can be used as

[170] *See, e.g.*, Richards, *supra* note 113, at 1955-56.

[171] *See* discussion *supra* Section I.C.

[172] ACLU Found. v. Superior Ct., 400 P.3d 432, 434 (Cal. 2017).

[173] *Id.* at 435. The agency didn't cite the state public records law privacy exemption. *See id.* at 436. Instead, it cited the investigatory exemption and a catchall balancing exemption. *Id.* But the catchall exemption analysis turned almost exclusively on the privacy interests involved. *Id.* at 439.

[174] *Id.* at 440.

[175] *Id.* at 442.

[176] *See, e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540, 658-63 (S.D.N.Y. 2013) (ordering body worn cameras in response to constitutional violations committed by the NYPD through their stop-and-frisk program).

evidence in a criminal prosecution, for example, or to support a police public relations campaign. And it allows them to withhold it from public view when the footage cut against police interests.[177]

In doing so, these agencies often rely on privacy-based arguments. The Oregon legislature, for example, amended its public records law in 2015 to require that all faces in police video cameras must be blurred prior to public disclosure.[178] Law enforcement officers testified in support of the bill, arguing that such protections were needed to shield both citizen and police officer's privacy.[179] The end result is that most agencies in the state must hand-redact body camera footage, which drives up the costs of producing such footage in the first place. Disclosure becomes so expensive that it acts as a barrier to obtaining body camera footage at all.[180]

Law enforcement agencies also invoke citizens' privacy interests to protect information about police contracts with the private sector, including private surveillance companies. Again, consider an example. Analysis of public records requests submitted to the NYPD through a website called MuckRock[181] shows that the agency has cited privacy exemptions to reject requests for contracts with

[177] *See* Jeffrey Bellin & Shevarma Pemberton, *Policing the Admissibility of Body Camera Evidence*, 87 FORDHAM L. REV. 1425, 1432 (2019) (describing this phenomenon); Umansky, *supra* note 143 (same).

[178] Act of June 25, 2015, ch. 550, § 5, Or. Laws 1329, 1337 (codified as amended and renumbered at OR. REV. STAT. ANN. § 192.345(40)(c) (West 2024)).

[179] *See* Letter from Daryl Turner, President, Or. Coal. of Police and Sheriffs, to Representatives Jeff Barker and Jennifer Williamson, Or. State Legislature (Apr. 29, 2015), https://olis.oregonlegislature.gov/liz/2015R1/Downloads/CommitteeMeetingDocument/75135 [https://perma.cc/N3W7-ERNH].

[180] *See* Claire Withycombe, *Police in Oregon: On-Body Cameras May Be Too Costly*, SEATTLE TIMES (July 12, 2015, 6:42 PM), https://www.seattletimes.com/seattle-news/police-in-oregon-on-body-cameras-may-be-too-costly/; *see also supra* notes 149-157 (describing examples of police withholding body camera footage on pretextual privacy grounds).

[181] For a discussion of this dataset, see *supra* note 132.

Palantir,[182] Clearview AI,[183] social media monitoring services,[184] and aerial drone providers.[185]

It is unclear why the records of contracts alone would implicate any privacy concerns. But even assuming there are legitimate privacy interests in shielding the substantive information gathered by third-party contractors, such protections still come at a cost. They prevent the public from learning about and ultimately contesting police reliance on these surveillance technologies and data aggregators. And they hinder the public's ability to organize against police data collection in the first place.

C. *Police Officer Privacy as Police Secrecy*

There is a second mechanism by which police use privacy interests to serve anti-accountability goals: police officer privacy protections. Police enjoy myriad privacy exemptions, many of them grounded in both safety and privacy concerns. These include, for instance, protections for police officers' addresses and phone numbers.[186] These provisions are narrow and targeted enough that they generally do not raise cooption concerns.

---

[182] *Compare, e.g.*, E-mail from Brendan O'Connor to NYPD (Mar. 7, 2016), https://www.muckrock.com/foi/new-york-city-17/palantir-nypd-24352/ [https://perma.cc/V2QV-XWRJ] (requesting "[c]opies of contracts with Palantir Technologies . . . and related services over the past 5 years"), *with* Letter from Richard Mantellino, Lieutenant, NYPD, to Brendan O'Connor (May 4, 2016), https://cdn.muckrock.com/foia_files/2016/05/13/5-4-16_MR24352_REJ-E_ID2016-PL-2816.pdf [https://perma.cc/3PWF-9TWS] (denying request under state's privacy exemption).

[183] *Compare* E-mail from Rachel Richards to NYPD (Aug. 28, 2020), https://www.muckrock.com/foi/new-york-city-17/clearview-ai-nypd-new-york-city-police-department-101653/ [https://perma.cc/5KMV-GLPU] (requesting emails containing terms "Clearview" and "Clearview licenses"), *with* E-mail from NYPD to Rachel Richards (Sept. 21, 2020), https://www.muckrock.com/foi/new-york-city-17/clearview-ai-nypd-new-york-city-police-department-101653/ [https://perma.cc/H4KG-A4CT] (denying request under state's privacy law exemption).

[184] *Compare* E-mail from Dell Cameron, Staff Rep., Daily Dot, to NYPD (June 27, 2017), https://www.muckrock.com/foi/new-york-city-17/nypd-social-media-services-39072/ [https://perma.cc/L46S-GPA7] (requesting purchasing agreements from social media monitoring companies), *with* Letter from Richard Mantellino, Lieutenant, Recs. Access Officer, NYPD, to Dell Cameron (Apr. 23, 2018), https://cdn.muckrock.com/foia_files/2018/04/30/4-23-18_MR39072_REJ_ID2017-PL-8712.pdf [https://perma.cc/TH7Z-49CB] (denying request in part under state's privacy law exemption).

[185] *Compare* Email from Shawn Musgrave to NYPD (Oct. 11, 2012), https://www.muckrock.com/foi/new-york-city-17/nyc-police-department-drone-documents-1985/ [https://perma.cc/KV9S-VPGQ], *with* Letter from Richard Mantellino, Lieutenant, Recs. Access Officer, NYPD, to Shawn Musgrave (Feb. 28, 2013), https://cdn.muckrock.com/foia_files/2-28-13_mr1985_REJ-V.pdf [https://perma.cc/6J8U-VUBY] (denying request under state's privacy law exemption).

[186] *See, e.g.*, MISS. CODE ANN. § 25-61-12(1) (2025); MICH. COMP. LAWS ANN. § 15.243(1)(s) (West 2025).

Yet among the strongest and broadest police officer privacy provisions are protections for police officers' disciplinary records. These carveouts, too, may be justified on due process and fairness grounds, especially when it comes to the disclosure of unsubstantiated complaints against police.[187] But privacy concerns are also a central justification for enacting such expansive disciplinary records' shields.[188]

Such protections are not exclusive to law enforcement officers. Many federal and state public records laws shield the personnel files of all government employees on privacy grounds.[189] There are also clear privacy justifications for doing so, including the risk of reputational harm.[190] But police are often granted additional protections, beyond those extended to other, nonpolice government employees, that cannot be supported by privacy considerations alone.

Consider the example of Delaware, which until recently had the nation's most protective disciplinary record regime.[191] The state's law shielded the files of any police officer who had been questioned "for any reason which could lead to disciplinary action, demotion, or dismissal."[192] These protections applied indefinitely, and they were difficult to overcome even with a showing of need.[193] The law was so protective that it shielded even anonymized information, including statistical summaries of completed internal affairs investigations.[194]

---

[187] For a discussion of these concerns, see Levine, *supra* note 27, at 870-79.

[188] *See* Moran, *supra* note 27, at 155 (citing California, Kentucky, and Hawaii as examples of privacy concerns being used to justify withholding misconduct records).

[189] FOIA, for example, excludes "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Some states have adopted similar language. *See supra* Part I.B.

[190] *See* Levine, *supra* note 27, at 886 (describing these privacy interests).

[191] *See Senate Sends Bills Revamping Law Enforcement Bill of Rights, Review Boards to Governor John Carney*, DEL. SENATE DEMOCRATS (June 30, 2023), https://senatedems.delaware.gov/2023/06/30/senate-sends-bills-revamping-law-enforcement-bill-of-rights-review-boards-to-governor-john-carney/ [https://perma.cc/BP7C-B26K] (noting in 2023 that "[d]isciplinary records for police officers recently convicted of domestic violence, sexual solicitation of a child, excessive force, abusing narcotics on the job and operating a phantom traffic ticket scheme are currently shielded from public view"). A new law provides public access to some substantiated complaints. *See* H.B. 205, 152d Gen. Assemb., Reg. Sess. (Del. 2023).

[192] DEL. CODE ANN. tit. 11, § 9200(d)(2) (2024).

[193] *See id.* (providing no time limit on disclosure); *see also* MO. ANN. STAT. § 590.502 (West 2024) (shielding "complete record of the administrative investigation" from disclosure absent subpoena or court order).

[194] *See* Michael Dworiak, No. 16-IB02 (Del. Off. Att'y Gen 2016), 2016 WL 1072888. Other states and agencies have withheld similar types of anonymized or aggregated disciplinary data. *See, e.g.*, N.Y. C.L. Union v. N.Y.C. Police Dep't, 118 N.E.3d 847, 855 (N.Y. 2018) ("FOIL's statutory scheme separately makes clear that redacted disclosure cannot be compelled where, as here, an agency has met its burden of demonstrating that records are

Such extensive protections for anonymized records cannot be grounded exclusively in privacy concerns. This is especially true when the disciplinary files of other, nonpolice government employees are not granted the same treatment.[195]

Exceptional secrecy protections contained outside of these statutory shields further undermine the privacy-based justifications. For example, many police contracts contain disciplinary protections that go beyond what other state or local government employees enjoy. Such provisions include requirements that police destroy disciplinary materials within a specified timeframe, sometimes as little as a few months.[196] They also include strict time limits for investigations—for instance, that complaints must be either substantiated within a short time window or dismissed.[197] These types of protections, too, are difficult to justify based on privacy concerns alone. Due process or fairness concerns may offer firmer grounding. But even these considerations cannot account for the discrepancies between the treatment of police versus nonpolice employees.

Police officer disciplinary files also hold information that is qualitatively different from the information contained in the files of other government

exempt from disclosure . . . ."); *see also* Jonathan Edwards, *Protesters Camp Out at Norfolk City Hall to Demand Police Release Use-of-Force Reports*, VIRGINIAN-PILOT, https://www.pilotonline.com/government/local/vp-nw-protesters-use-of-force-20200630-64455u5idndrdhad3237jwsvk4-story.html (last updated June 30, 2020, 11:20 PM) (describing police department's refusal to release deidentified use of force reports).

[195] *See, e.g.*, DEL. CODE ANN. tit. 29, § 10002(o) (2024) (outlining reducing privacy protections for public access to nonpolice government personnel records); MO. REV. STAT. § 590.502 (2024) (protecting only law enforcement disciplinary files from disclosure); LA. STAT. ANN. § 40:2532 (2024) (requiring that police provide "written consent" before information about an investigation into the officer is released to the press). Other interests may account for such distinctions. For example, police unions often argue that there are heightened concerns about retaliation against police officers. *See, e.g.*, Press Release, NYC PBA, Statement on 50-a Repeal (June 10, 2020), https://www.nycpba.org/press-releases/2020/nyc-pba-statement-on-50-a-repeal/ [https://perma.cc/KEW4-XKXX] (opposing repeal of Section-50a on officer safety grounds). There is little empirical evidence to support these claims. Moran, *supra* note 27, at 196 ("The notion that disclosure of police records encourages or enables retaliation by the public against officers is, as criminology professor John Worrall has noted, based on a 'total lack of data.'"). But even if there were, options like the release of redacted files could help assuage them. Laws like Delaware's don't permit any disclosure at all. *See supra* notes 194-195.

[196] *See* Reade Levinson, *Across the U.S., Police Contracts Shield Officers from Scrutiny and Discipline*, REUTERS (Jan. 13, 2017, 1:18 PM), https://www.reuters.com/investigates/special-report/usa-police-unions/ (stating majority of the eighty-two police union contracts in large cities surveyed require erasure of disciplinary records, some after six months).

[197] *Id.* (stating seventeen cities set time limits for citizens to files complaints, some as short as thirty days).

workers.[198] Information about police uses of force, police killings, and police abuse of power is often located within the disciplinary files of individual officers.[199] As a result, privacy-based exemptions operate to prevent the victims of police violence from learning what happened. The mother of Eric Garner, the man who was choked to death by an NYPD officer in 2014, emphasized this in her testimony before the New York State legislature. "We should know firsthand when our loved ones are killed," she stated.[200] "We should know who did it, why they did it, and . . . all the details. . . . But this is hidden because of 50-a," referring to the New York police privacy law.[201]

Such files also contain impeachment evidence that can be used by criminal defendants. In some states, prosecutors are relieved of their *Brady* obligations if these disciplinary materials are made available to defendants under public records statutes.[202] Such evidence is also crucial for plaintiffs in civil rights cases against police. Further, such records can shed light on police violence nationwide. Police departments often fail to report this data to the FBI.[203] As a result, the most comprehensive police use of force and police killing databases in the nation have been created by nongovernmental actors like newspapers and

[198] *See, e.g.*, Great Falls Trib. Co. v. Cascade Cnty. Sheriff, 775 P.2d 1267, 1269 (Mont. 1989) ("[L]aw enforcement officers occupy positions of great public trust. . . . [T]he public has a right to know when law enforcement officers act in such a manner as to be subject to disciplinary action.").

[199] *See, e.g.*, Levine, *supra* note 27, at 862-64 (providing example "discipline matrix" from Madison, Wisconsin, that contains section for use of force violations).

[200] Jeff Coltin & Amanda Luz Henning Santiago, *A Guide to 50-a, the Most Contentious State Law on the Books*, CITY & STATE N.Y. (Oct. 18, 2019), https://www.cityandstateny.com/policy/2019/10/a-guide-to-50-a-the-most-contentious-state-law-on-the-books/177365/ [https://perma.cc/539B-P7DR].

[201] *Id.*; *see also* Umar Farooq, *When Alabama Police Kill, Surviving Family Can Fight Years to See Bodycam Footage. There's No Guarantee They Will.*, PROPUBLICA (Dec. 28, 2023, 5:00 AM), https://www.propublica.org/article/police-body-camera-footage-alabama-restrictions [https://perma.cc/4NS7-TFNX] (describing how relatives of those killed by police battle for access to body camera footage of killing).

[202] *See* Jonathan Abel, Brady*'s Blind Spot: Impeachment Evidence in Police Personnel Files and the Battle Splitting the Prosecution Team*, 67 STAN. L. REV. 743, 770-73 (2015).

[203] *See* Tom Jackman, *For a Second Year, Most U.S. Police Departments Decline to Share Information on Their Use of Force*, WASH. POST (June 9, 2021), https://www.washingtonpost.com/nation/2021/06/09/police-use-of-force-data/.

activist organizations using public records laws.[204] For these reasons, the stakes are especially high when it comes to accessing police disciplinary materials.[205]

But precisely because these privacy-based protections shield officer misconduct, they are often coopted to serve anti-accountability ends.[206] Occasionally, this point is made explicit. New York's highest court, for example, once stated that the purpose of the state's former shield for police disciplinary records was to prevent criminal defense attorneys from abusing these personnel files during the cross-examination of police.[207] The statutory protections in force at the time shielded even substantiated claims against officers, so concerns about unfair reputational damage alone could not account for the breadth of this protection.[208] It was an unusually candid admission that preventing scrutiny of the officers was the point of these privacy-based shields.[209]

Police unions also justify these strong protections on explicitly anti-accountability grounds. In 2017, for example, the general counsel for the Maryland Chiefs of Police opposed a proposed bill to expand public access to police disciplinary records on the grounds that it would create "intrusive opportunities to challenge a chief or sheriff's decision-making process."[210] Other police officials or union representatives have advanced similar claims.[211]

---

[204] Even the FBI has admitted that the *Washington Post* has a more accurate police use of force database than the agency does. *See* Aaron C. Davis & Wesley Lowery, *FBI Director Calls Lack of Data on Police Shootings 'Ridiculous,' 'Embarrassing*,*'* WASH. POST (Oct. 7, 2015), https://www.washingtonpost.com/national/fbi-director-calls-lack-of-data-on-police-shootings-ridiculous-embarrassing/2015/10/07/c0ebaf7a-6d16-11e5-b31c-d80d62b53e28_story.html.

[205] *But see* Levine, *supra* note 27, at 872-80 (questioning value and benefits of making police disciplinary files public).

[206] As a threshold matter, there is the question of whether these disciplinary files contain any legitimately private information at all. *See* Moran, *supra* note 27, at 177-78 (arguing these files mostly contain information that historically has not been considered private).

[207] Daily Gazette Co. v. City of Schenectady, 710 N.E.2d 1072, 1075 (N.Y. 1999).

[208] *See* COMM. ON OPEN GOV'T, N.Y. STATE DEP'T OF STATE, 2018 REPORT TO THE GOVERNOR AND STATE LEGISLATURE 4 (2018) (noting Section 50-a makes confidential even substantiated claims against police, which "defeats the objectives of FOIL and serves no apparent compelling policy purpose"). Section 50-a has since been repealed. N.Y. CIV. RIGHTS LAW § 50-a (McKinney 2020), *repealed by* Act of June 12, 2020, ch. 96, § 1, 2020 N.Y. Laws 780, 780.

[209] Some judges have gone even further. *See, e.g.*, Campbell v. U.S. DOJ, 193 F. Supp. 2d 29, 40-41 (D.D.C. 2001) (holding pervasive police misconduct during McCarthy era was one reason to enhance privacy protections for law enforcement officers involved).

[210] *See* Justin Fenton, *Baltimore Police Disciplinary Records Remain Shielded Despite Revelations of Misconduc*t, BALT. SUN, https://www.baltimoresun.com/news/crime/bs-md-ci-police-records-transparency-20180214-story.html (last updated June 30, 2019, 8:00 PM).

[211] For example, the (then) head of the Police Benevolent Association of the City of New York, President Patrick Lynch, opposed a proposed bill imposing new transparency measures on the grounds that "[p]olicing policies must be left to the police management who understand

From this perspective, the oversight barriers imposed by these privacy shields are seen as a benefit, rather than a cost.[212]

Further, law enforcement agencies not only invoke exclusive privacy protections denied to other government actors, but they also utilize privacy shields intended to apply to the public at large. One example is police reliance on Marsy's Law provisions, or constitutional provisions adopted by roughly a dozen states to shield the information of crime victims from public disclosure.[213] In their original forms, these state constitutional provisions shielded confidential crime victim information only when it was being requested by the alleged perpetrator.[214] But in a handful of states, this original language has been amended or interpreted to prevent disclosure of crime victim information to anyone at all.[215] As a consequence, law enforcement agencies in these states

the intricacies and difficulties of complex legal issues and the appropriate use of crime-fighting tactics." Michael Gartland, *Cops Livid over Proposed 'Police Reform' Measures*, N.Y. POST (June 29, 2015, 12:25 AM), https://nypost.com/2015/06/29/cops-livid-over-proposed-police-reform-measures/ [https://perma.cc/QU2W-PNA4].

[212] Law enforcement officers may also coopt privacy claims by defining the scope of personnel records very broadly. *See, e.g.*, Tim Hrenchir, *Topeka Police Refuse to Release Body Camera Footage of June Fatal Officer-Involved Shooting*, TOPEKA CAP.-J. (Oct. 3, 2022, 10:16 AM CT), https://www.cjonline.com/story/news/local/2022/10/03/topeka-police-release-body-camera-video-fatal-officer-involved-shooting-christopher-kelley/69529825007/ [https://perma.cc/KY53-3P7Z] (describing Topeka Police Department withholding body camera recording of fatal police shooting on grounds it was personnel record).

[213] *See* Paul G. Cassell & Margaret Garvin, *Protecting Crime Victims in State Constitutions: The Example of the New Marsy's Law for Florida*, 110 J. CRIM. L. & CRIMINOLOGY 99, 101 (2020).

[214] *See* CAL. CONST. art. I, § 28 ("In order to preserve and protect a victim's rights to justice and due process, a victim shall be entitled to . . . prevent the disclosure of confidential information or records to the defendant . . . ."); *see also* GA. CONST. art. I, § 1, ¶ XXX; ILL. CONST. art. I, § 8; KY. CONST. § 26A; N.C. CONST. art. I, § 37; NEV. CONST. art. I, § 8A; OHIO CONST. art. I, § 10a; OKLA. CONST. art. II, § 34; WIS. CONST. art. I, § 9m(2).

[215] *See* FLA. CONST. art. I, § 16(b) (granting crime victims "[t]he right to prevent the disclosure of information or records that could be used to locate or harass the victim or the victim's family, or which could disclose confidential or privileged information"); N.D. CONST. art. I, § 25; S.D. CONST. art. VI, § 29. In Ohio, the statutory language was amended to create a similarly broad shield. OHIO REV. CODE ANN. § 2930.07(C)-(D) (LexisNexis 2025); *see also* Kenny Jacoby & Ryan Gabrielson, *How Cops Who Use Force and Even Kill Can Hide Their Names from the Public*, PROPUBLICA (Oct. 29, 2020, 6:00 AM), https://www.propublica.org/article/how-cops-who-use-force-and-even-kill-can-hide-their-names-from-the-public [https://perma.cc/Q2Z9-BQBR] ("[O]nly in Florida, North Dakota and South Dakota can police officers use the law to shield their names from the public.").

have widely invoked this provision to shield the names of police officers accused of wrongdoing, including those involved in the killing of civilians.[216]

Two categories of Marsy's Law protections for police have become especially contested. The first involves law enforcement agencies' reliance on victims' rights provisions to withhold the names of law enforcement officers involved in serious acts of violence. In these instances, police officers kill someone, and then they argue they are the victims of crimes committed against them by the deceased.[217] As a result, the police officers argue, their own names must be protected from public disclosure.

In Ohio, for example, a police officer shot and killed a pregnant woman in August 2023.[218] The police department then refused to release the name of the officer under Marsy's Law. It argued that the pregnant woman had slowly rolled her car toward the officer before she was shot, and therefore the officer was the victim of an automotive assault.[219]

---

[216] *See, e.g.*, Jeanne Hruska & Janna Farley, *In South Dakota, Police Officers Involved in Shootings Are Claiming They Have a Right to Privacy as Crime Victims*, ACLU (Dec. 27, 2018), https://www.aclu.org/news/criminal-law-reform/south-dakota-police-officers-involved-shootings [https://perma.cc/6Q6A-L59W].

[217] *See Herald Asks for Clarity on Marsy's Law*, GRAND FORKS HERALD (May 25, 2017), https://www.grandforksherald.com/newsmd/herald-asks-for-clarity-on-marsys-law [https://perma.cc/HSB6-JXKU?type=image] (describing withholdings under Marsy's Law in North Dakota); Ed Lyon, *Under Marsy's Law, Police Using Violence Can Claim 'Victim' Status*, CRIM. LEGAL NEWS (July 17, 2019), https://www.criminallegalnews.org/news/2019/jul/17/under-marsys-law-police-using-violence-can-claim-victim-status/ [https://perma.cc/UVS6-QKEV]; Matthew Harwood, *Marsy's Law Is a Gift to Bad Cops*, REASON (Mar. 18, 2019, 9:45 AM), https://reason.com/2019/03/18/marsys-law-is-a-gift-to-bad-cops/ [https://perma.cc/XH2T-C3GC] (describing withholdings under Marsy's Law in South Dakota); Jamiles Lartey, *When Police Kill and Use Victims' Rights Laws to Stay Anonymous*, MARSHALL PROJECT (Sept. 9, 2023, 12:00 PM), https://www.themarshallproject.org/2023/09/09/ohio-police-crime-victim-law [https://perma.cc/JXH2-XPAC] (describing withholdings under Marsy's Law in Ohio); Jacob Resneck, *Oshkosh Police Cite 'Marsy's Law' to Withhold Names of Officers Who Shot Suspects*, WIS. WATCH (Aug. 8, 2023), https://wisconsinwatch.org/2023/08/oshkosh-police-marsys-law-withhold-names-of-officers-who-shot-suspects/ [https://perma.cc/9572-RNHL] (describing withholdings under Marsy's Law in Wisconsin).

[218] Lartey, *supra* note 217.

[219] *Id*. ("As far as the justice system is concerned, there are two crime victims in the case, but perhaps not the two you might expect. . . . The officer who fired, and another who was nearby, are being treated as the victims of an automotive assault . . . ."). Police departments in the state have refused to release other body camera recordings of police shootings on similar grounds. Bethany Bruner, *Columbus City Attorney Explains Why Names, Bodycam Video from Police Shootings Is Limited*, COLUMBUS DISPATCH, https://eu.dispatch.com/story/news/crime/2023/07/13/city-attorney-explains-limited-body-camera-from-shootings-columbus-ohio-zach-klein-marsys-law/70410462007/ [https://perma.cc/828S-QUKD] (last updated July 14, 2023, 5:58 PM). At the same time, the department has released body camera footage of acts of violence against police that did not result in fatal police shootings. *Id.*

Similarly, in Florida, a police officer tried to pull over a thirteen-year-old who was riding a dirt bike.[220] The bike crashed, and the child died. The police officer argued their name could not be released to the public because the officer received threats over their involvement in the child's death, and therefore they had become a victim of a crime under Marsy's Law.[221]

In some places, Marsy's Law has been invoked to shield almost all police uses of force from public view. The Supreme Court of Florida recently held that the constitutional provision does not permit victims an absolute right to withhold their names from public disclosure.[222] Yet prior to that decision, police departments across the state relied on Marsy's Law for years to withhold the names of police officers who killed or seriously injured civilians. The Jacksonville Sheriff's Office, for instance, withheld the name of every police officer involved in a shooting from January 2019 to August 2021 under Marsy's Law—fifty-nine in total.[223] It maintained that each of these officers was a victim of a crime.[224] Likewise, in a county near Tampa, the police department invoked Marsy's Law to shield the officer's name in one out of three police uses of force that resulted in injury to a civilian.[225]

The second category of contentious Marsy's Law protections involves police officers' use of victims' rights protections when the harm committed against officers is minimal or nonexistent. In 2019, for example, a handcuffed man swung an object in the direction of a police officer.[226] The officer pepper sprayed the man. The officer then argued that he was the victim of an assault by the handcuffed man, and therefore the officer's name should be withheld under Marsy's Law.[227]

A joint investigation by *ProPublica* and *USA Today* uncovered dozens of such low-level threats against police officers under which the officers claimed victim status.[228] These included claims that behavior by citizens such as

[220] *See* Andrew Lofholm, *Should Police Officers Be Protected by Marsy's Law?*, CBS12 NEWS, https://cbs12.com/news/local/should-police-officers-be-protected-by-marsys-law-stanley-davis-deadly-dirt-bike-crash-boynton-beach [https://perma.cc/W5B8-4D3B] (last updated Jan. 26, 2022, 5:20 PM).

[221] *Id.*

[222] City of Tallahassee v. Fla. Police Benevolent Ass'n, 375 So. 3d 178, 181 (Fla. 2023). A challenge was recently filed in Ohio as well. *See* Complaint for Writ of Mandamus at 4, State *ex rel.* Gatehouse Media Ohio Holdings II, Inc. v. City of Columbus, No. 2023-1327 (Ohio Oct. 19, 2023).

[223] Uriel J. Garcia, *Marsy's Law Was Supposed to Help Victims. In Jacksonville, It Shields Police Officers.*, TRIBUTARY (Aug. 3, 2021), https://jaxtrib.org/2021/08/03/jacksonville-police-shootings/ [https://perma.cc/VB4B-5U8V].

[224] *Id.*

[225] *See* Jacoby & Gabrielson, *supra* note 215.

[226] *Id.*

[227] *Id*.

[228] *See id.* ("Sometimes, the injuries officers cited when they invoked the victim status were as minor as a scraped knee, soreness or a twisted wrist.").

"walking aggressively or reaching into a pocket" allowed police to claim victim status.[229] Such claims have permitted police in these states to withhold huge swaths of information over police use-of-force and other records.[230]

There are two central ways that privacy cooption may be implicated in these police victim claims. The first is that voters did not intend for law enforcement officers acting within the scope of their official duties to be classified as crime "victims."[231] In Florida, for example, the ballot summary for the proposed Marsy's Law amendment did not include a definition of "victims' rights."[232] And the original sponsor of the amendment—a county sheriff—suggested in a statement before the state's Constitutional Revision Commission that such protections were not intended to apply to police.[233]

Moreover, the explicit intent of these laws is to "ensure a meaningful role" for crime victims "throughout the criminal and juvenile justice systems."[234] As Professor Nadia Banteka has noted, police officers already play a role in the criminal justice system, in numerous ways.[235] Extending such protections to police therefore contradicts the original justifications that motivated Marsy's Law protections.[236]

Second, even assuming that the plain language of the law encompasses on-duty law enforcement officials, many of these Marsy's Law claims are doubtful

[229] *Id.*

[230] *Id.* Victims' rights statutes enacted in other states provide similar protections. *See, e.g.*, VA. CODE ANN. § 2.2-3706(B) (2024) (declaring most records of law enforcement agencies and identities of victims are "discretionary releases"); *see also* Tom Jackman, *Va. Seeks Records Law Change to Require Victim Notification Before Releasing Crime Files*, WASH. POST (Mar. 11, 2022), https://www.washingtonpost.com/dc-md-va/2022/03/11/va-foia-change/ (describing concerns that statutory victims' rights provisions will be used by police "to deny access to virtually all of their files, from all requesters").

[231] Courts in at least two states enjoined Marsy's Law protections from going into effect because the wording on the ballot was so confusing. *See* League of Women Voters of Pa. v. DeGraffenreid, 265 A.3d 207, 210 (Pa. 2021); Mont. Ass'n of Cntys. v. State *ex rel.* Fox, 2017 MT 267, ¶¶ 3, 5, 389 Mont. 183, 185-86, 404 P.3d 733, 735-36. *But see* Dep't of State v. Hollander, 256 So. 3d 1300, 1302 (Fla. 2018) (rejecting claim that Marsy's Law ballot title and summary were misleading); Wis. Just. Initiative, Inc. v. Wis. Elections Comm'n, 2023 WI 38, ¶¶ 5, 7, 407 Wis. 2d 87, 94-96, 990 N.W.2d 122, 126-27 (same).

[232] *Hollander*, 256 So. 3d at 1308.

[233] *See* ACLU of Florida's Amicus Curiae Brief Supporting Petitioner City of Tallahassee and Intervenors News Media Coalition at 2, City of Tallahassee v. Fla. Police Benevolent Ass'n, 375 So. 3d 178, No. SC21-651 (Fla. 2023) (citing county sheriff's statement that "protections were needed because crime victims' role in the criminal justice system—in contrast to 'cops [like himself],' who 'wear a uniform [and] go to work every day'—is unchosen").

[234] *See, e.g.*, FLA. CONST. art. I, § 16(b). Other laws contain variations on this language. *See, e.g.*, OHIO CONST. art. I, § 10a(A).

[235] Banteka, *supra* note 28, at 1897.

[236] *Id.*

on their face. It is implausible that every single police officer involved in a shooting over the course of years was the victim of a crime.[237] It also strains credulity that police would require privacy protections for something like someone walking aggressively towards them. Police are coopting provisions intended to protect victims' privacy to shield their own activities from public view.

D. *The Mechanisms of Privacy Cooption*

There are inherent privacy-accountability tensions embedded within transparency laws.[238] Such trade-offs are unavoidable. Most jurisdictions have dealt with this tension by establishing a balancing test that weighs the individual's privacy interests against the public's interest in disclosure.[239] Yet in the context of policing, the privacy side of the balance is often stacked in the police's favor and filled with vague and broad exemptions that are easily coopted for other ends. It is impossible to give a full or definitive account of the potential drivers of this process. But there are a number of possible explanations.

First, legislatures contribute to police privacy cooption. Under FOIA and some state public records laws, a different privacy-accountability balance has been struck for police records. These statutes permit law enforcement agencies to meet a lower threshold of privacy harm before they withhold a record from public view.[240] This balancing test is weighted from the start in favor of police secrecy. Yet the justifications for doing so are flawed. The reason most often given is that individuals have an especially strong interest in not being associated with criminal activity.[241] But the traditional balancing test applicable to all other agencies already permits the decisionmaker to take such considerations into account.[242] It is unclear why the standard balancing test applicable to other agencies is insufficient to account for such concerns.

---

[237] *See supra* note 224 and accompanying text.

[238] *See* Solove, *supra* note 30, at 1140 (describing this tension).

[239] *See, e.g.*, Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157, 171 (2004) ("The term 'unwarranted' requires us to balance the family's privacy interest against the public interest in disclosure."); Int'l Fed'n of Pro. & Tech. Eng'rs, Loc. 21 v. Superior Ct., 165 P.3d 488, 493 (Cal. 2007) ("This exemption requires us to balance two competing interests, both of which the Act seeks to protect—the public's interest in disclosure and the individual's interest in personal privacy.").

[240] 5 U.S.C. § 552(b)(7) (allowing withholding of law enforcement records and information to extent they "could reasonably be expected to constitute an unwarranted invasion of personal privacy"); ALASKA STAT. § 40.25.120(a)(6)(C) (2025); IDAHO CODE § 74-124 (2025); MD. CODE ANN., GEN. PROVIS. § 4-351 (LexisNexis 2024) (bestowing broad discretion to law enforcement, including ability to deny inspection of records compiled for law enforcement purpose and records pertaining to investigations of police misconduct, subject to few caveats); MICH. COMP. LAWS ANN. § 15.243 (West 2025); S.C. CODE ANN. § 30-4-40 (West 2025); VT. STAT. ANN. tit. 1, § 317 (2025).

[241] *See, e.g.*, Fitzgibbon v. CIA, 911 F.2d 755, 767 (D.C. Cir. 1990).

[242] *See supra* note 239 and accompanying text.

Second, the courts act as a driver of cooption. Judges are especially quick to defer to law enforcement agencies' assertions of harm.[243] And they often feel ill-equipped to overrule police departments' claims about the risks of information disclosures.[244] Courts have made this explicit when it comes to national security information disclosures.[245] But these claims have increasingly made their way into policing as well.[246] The "mosaic theory" of information disclosure has proven especially persuasive. The theory holds that technological advances allow observers to gather various nonsensitive facts and infer from them sensitive information.[247] The theory originated in support of national security secrecy.[248] But increasingly, it has surfaced in the law enforcement context as well.[249]

Such concerns may be legitimate, especially in light of rapid advances in artificial intelligence.[250] The fear is that machine learning and other techniques will permit an observer to infer sensitive facts from a collection of nonsensitive ones. But the remedy is not to shut down public access altogether, especially in the context of policing. Doing so would create perverse incentives: Under this logic, the more information police are able to gather, the more persuasive their mosaic theory arguments against disclosure become. An ever-expanding amount of agency activity would be shielded from public view, and increased surveillance of the public would necessarily mean increased barriers against

[243] *See* Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. REV. 185, 216-19 (2013).

[244] *See, e.g.*, N.J. Media Grp., Inc. v. Ashcroft, 308 F.3d 198, 219 (3d Cir. 2002) ("[G]iven judges' relative lack of expertise regarding national security and their inability to see the mosaic, we should not entrust to them the decision whether an isolated fact is sensitive enough to warrant closure.").

[245] *See, e.g.*, Stein v. U.S. DOJ, 662 F.2d 1245, 1254 (7th Cir. 1981) ("[Courts] must defer to the agency's evaluation of the need to maintain the secrecy of the methods used to carry out such [classified] projects.").

[246] *See, e.g.*, Ctr. for Nat'l Sec. Stud. v. U.S. DOJ, 331 F.3d 918, 928 (D.C. Cir. 2003) (extending deference afforded under Exemption 1, which shields information made classified by Executive Order, to Exemption 7, which shields law enforcement records); *see also* Christina Koningisor, *Secrecy Creep*, 169 U. PA. L. REV. 1751, 1785-87 (2021).

[247] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 633-34 (2005).

[248] *See id.*

[249] Abdur-Rashid v. N.Y.C. Police Dep't, 100 N.E.3d 799, 811 (N.Y. 2018) (relying on mosaic theory to justify permitting NYPD to issue so-called "Glomar response," refusing to confirm or deny existence of records).

[250] *See, e.g.*, Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081, 1083-84 (2024) (emphasizing how modern technology facilitates process of making inferences about sensitive data from disclosures of non-sensitive data).

public oversight. This approach would incentivize police to gather data precisely for its secrecy-expanding effects.[251]

A better solution would be to reduce government surveillance and create better regulatory solutions to the problem of inferences. Privacy law scholar Paul Ohm has argued for laws regulating the processing of data that "reveals" sensitive information, much like the approach embodied in Europe's GDPR.[252] Recipients using public records statutes to obtain police records could be equally bound by such laws. Moreover, the apparent alternative is to abandon public oversight mechanisms and permit government actors to withhold an ever-growing body of information on privacy grounds.[253] This cannot be the solution.

Courts have also construed the privacy-accountability trade-offs in ways that facilitate privacy cooption. Again, most public records laws require that an agency weigh the individual's interest in keeping the information private against the strength of the public's interest in disclosure.[254] This general approach makes sense: It permits the decisionmaker to take both these competing values into consideration. Yet the courts have interpreted and applied these requirements in secrecy-enhancing ways.

On the privacy side, courts have defined "privacy" broadly. The federal courts have held that privacy encompasses "the prosaic (e.g., place of birth and date of marriage) as well as the intimate and potentially embarrassing."[255] They have also held, somewhat counterintuitively, that "[a] substantial privacy interest is anything greater than a *de minimis* privacy interest."[256] There are privacy benefits to such an expansive approach. But there are also accountability costs. Redacting files is expensive and time consuming, and agencies are often reluctant to do so.[257] Moreover, courts rarely step in to enforce redaction and disclosure obligations.[258] As a result, when privacy protections attach to mundane bureaucratic information like signatures or email addresses, law

[251] Professor Nadia Banteka tells a different story of legal drift, one which contends that the Court's acceptance of police pretexts in *Whren v. United States*, 517 U.S. 806, 813 (1996), sent a message that pretextual claims by police would be accepted more broadly. *See* Banteka, *supra* note 28, at 1890-91 (citing *Whren*, 517 U.S. at 813) (describing how Court's condoning use of pretext in searches "spread into how entire departments conceived of and represented officers to the public").

[252] *See* Ohm, *supra* note 57, at 29-30.

[253] *Id.* at 9-11.

[254] *See supra* notes 63-66.

[255] Painting & Drywall Work Pres. Fund, Inc. v. Dep't of Hous. & Urb. Dev., 936 F.2d 1300, 1302 (D.C. Cir. 1991).

[256] Multi Ag Media LLC v. Dep't of Agric., 515 F.3d 1224, 1229-30 (D.C. Cir. 2008).

[257] Laurence Tai, *Fast Fixes for FOIA*, 52 HARV. J. ON LEGIS. 455, 461-62 (2015).

[258] *See, e.g.*, Margaret B. Kwoka, *Deference,* Chenery*, and FOIA*, 73 MD. L REV. 1060, 1073 (2014) (analyzing courts' highly deferential review of FOIA request denials).

enforcement agencies operating in bad faith obtain a powerful tool of nondisclosure.[259]

Courts have also held that the privacy interests of a government employee increase the lower the individual sits within an organizational hierarchy. In other words, lower-level employees are presumed to have greater privacy interest than higher-level ones.[260] Again, it makes some sense to enshrine institutional power imbalances into the law in this way. Yet this approach also ignores certain functional realities in the context of policing. Individual police officers are often lower down the organizational chart, for example, and yet they wield substantial authority and power over the public. This rule can operate as an impediment to disclosure when low-level employees nonetheless abuse their positions.

On the public interest side of the balance, in contrast, courts have also adopted a narrow interpretation of the interests that may be vindicated. The federal courts have not accepted criminal defendants' claims that the public interest is served by disclosing records that would be useful to them in mounting their defense, for instance.[261] They have also rejected arguments that there is a public interest in obtaining federal agency records that reveal state agency wrongdoing.[262] Such cramped interpretations of the public interest side of the balance facilitate privacy cooption as well.

Finally, law enforcement agencies themselves drive cooption. Police departments and police unions are politically powerful.[263] And state and local governments often face budgetary constraints that make it difficult to increase police officer pay. As a result, civilian leaders often make non-monetary concessions during contract negotiations, including extending broad police officer information shields under the guise of privacy.[264] As discussed above, such provisions have substantial anti-accountability effects.[265] Even if such provisions are rooted in part in privacy concerns, they far exceed what other government employees enjoy.[266] They also exceed the protections granted to civilians similarly accused of crimes.[267] This suggests that such protections may

[259] *See, e.g.*, CPD MuckRock Data, *supra* note 132 (showing that CPD routinely withholds signatures and email addresses under state public records exemption for private information).

[260] *See, e.g.*, U.S. DOJ, GUIDE TO THE FREEDOM OF INFORMATION ACT: EXEMPTION 6, at 66-70 (2025), https://www.justice.gov/oip/page/file/1207336/dl [https://perma.cc/H7L5-PLPV] ("Many courts have focused in particular on the employee's rank, identifying less public interest in both serious and less serious misconduct by lower-level agency employees.").

[261] *See infra* notes 346-347.

[262] Landano v. U.S. DOJ, 956 F.2d 422, 430 (3d Cir. 1992).

[263] Catherine L. Fisk & L. Song Richardson, *Police Unions*, 85 GEO. WASH. L. REV. 713, 744-47 (2017).

[264] *See* Stephen Rushin, *Police Union Contracts*, 66 DUKE L.J. 1191, 1245-47 (2017) (discussing how Chicago officials offered lenient disciplinary procedures in exchange for lower police salaries during contract negotiations).

[265] *See* discussion *supra* Section II.C.

[266] *See* discussion *supra* Section II.C.

[267] *See* discussion *supra* Section II.C (detailing disciplinary exceptions for police officers).

be driven at least in part by anti-accountability motivations, rather than genuine privacy concerns.

III. THE HARMS OF PRIVACY COOPTION

Police records contain troves of sensitive data. Police intervene in difficult moments of people's lives, and the records they create capture these intimate details.[268] Police personnel records contain information about police officers' physical and mental health.[269] Criminal justice records contain private information about the victims of a crime. And programmatic surveillance efforts hold vast troves of data about the public at large.[270] Police records contain sensitive information, and there are strong reasons to protect them from unnecessary disclosure.

Such benefits are myriad. These privacy protections allow those who have been arrested or convicted to have a fresh start.[271] They offer protection for victims who do not want information about the crimes committed against them to be made public.[272] And they protect the communities that have been subjected to the most frequent and heavy police surveillance.[273] As long as police are permitted to gather large amounts of sensitive data, privacy safeguards are needed.

Yet there are also costs to these expansive privacy shields. The lens of privacy cooption helps to bring these harms into focus. The current legal approach privileges protection against certain types of privacy intrusions—such as the public dissemination of private information—over others, such as the collection of private data by government actors. These protections are often distributed unequally, deployed to protect the privacy of police officers and their political allies while exposing information about the communities most subjected to pervasive and abusive policing. And they impede democratic processes, making

[268] Such privacy concerns animate debates over whether categories of records like 911 call recordings and transcripts should be released, for example. *See, e.g.*, ALA. CODE § 11-98-12 (2025) (prescribing that recordings may only be released if public interest outweighs individual's privacy interests); A.H. Belo Corp. v. Mesa Police Dep't, 42 P.3d 615, 618 (Ariz. Ct. App. 2002) (concluding that privacy interests of injured child outweigh public's interest in disclosure of 911 tape).

[269] *See* Moran, *supra* note 27, at 179-80 (describing examples of medical records contained in police personnel files).

[270] *See, e.g.*, *supra* notes 174-75 and accompanying text (describing privacy interests in ALPR data).

[271] *See, e.g.*, N.Y. CRIM. PROC. LAW § 160.50 (McKinney 2025) (providing for automatic sealing of criminal proceedings that end in favor of the accused).

[272] *See, e.g.*, discussion *supra* note 214 and accompanying text (describing Marsy's Law protections).

[273] *See* SIMONE BROWNE, DARK MATTERS 9-10 (2015) (discussing historic and modern surveillance of Black people); Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016, 5:55 AM), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.

it more difficult for the public to learn about and contest police action. This next Part surveys these harms.

A. *Privacy Harms*

The tension between privacy and other values—transparency,[274] free speech,[275] democratic accountability,[276] security,[277] and so on—is well documented in the literature.[278] Stronger privacy protections against police surveillance, for example, may make it more difficult for police to detect security threats.[279] Legislators and judges consistently weigh these benefits and costs. And yet the present information-access regime also embodies a trade-off between distinct privacy values—what Professor David Pozen has referred to as "privacy-privacy tradeoffs."[280]

Judges, scholars, and policymakers have long sought to identify, catalogue, and measure these different types of privacy harms.[281] Many approaches have been offered, each with its own advantages and drawbacks.[282] But Professor Daniel Solove's influential 2006 article *A Taxonomy of Privacy* offers a useful

[274] *See, e.g.*, Moran, *supra* note 27, at 154-56 (describing tensions between transparency and privacy in disclosing police disciplinary files).

[275] *See, e.g.*, Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 402 & n.92 (2008) (listing works that "accept[] the basic proposition that privacy and free speech are competing values"); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000) ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.").

[276] *See, e.g.*, 5 U.S.C. § 552(b)(6) (exempting certain records that contain private information from public disclosure).

[277] *See, e.g.*, Kenneth Einar Himma, *Privacy Versus Security: Why Privacy Is Not an Absolute Value or Right*, 44 SAN DIEGO L. REV. 857, 859-60 (2007) (examining trade-offs between privacy and security through lens of philosophy).

[278] *See* Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1904 (2013) ("[W]hen privacy and its purportedly outdated values must be balanced against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser."); Angel & Calo, *supra* note 116, at 542-46 (summarizing feminist and LGBT critiques to privacy law).

[279] This reasoning leads to many police surveillance abuses. *See generally* MATT APUZZO & ADAM GOLDMAN, ENEMIES WITHIN: INSIDE THE NYPD'S SECRET SPYING UNIT AND BIN LADEN'S FINAL PLOT AGAINST AMERICA (2013) (describing how concerns about terrorism threats motivated NYPD to violate Muslim-Americans' privacy in massive surveillance operation).

[280] Pozen, *supra* note 34, at 222 ("[I]n myriad social and regulatory contexts, enhancing or preserving privacy along a certain axis may entail compromising privacy along another axis.").

[281] *See* Angel & Calo, *supra* note 116, at 512 (describing some of these approaches).

[282] *See id.* at 509 ("A parade of articles and books, from *The Right to Privacy* [in 1890] onward, offered varying definitions for [privacy].").

framework to compare different types of privacy.[283] In doing so, it reveals how the current privacy law regime imposes a specific set of privacy-privacy tradeoffs.[284]

In his article, Professor Solove outlines four types of activity affecting privacy. The first is information collection, which encompasses activities like surveillance and interrogation.[285] The second is information processing, which pertains to the management of collected data and includes activities like data aggregation and secondary use of information.[286] The third is information dissemination, which involves broader disclosures of data that has already been gathered and processed.[287] And the fourth is invasion, or activities that disturb an individual's "right to be let alone," such as searching one's home or interfering with one's intimate bodily decisions.[288] This final category plays less of a role in the police records privacy regime.[289] But the first three categories are helpful in thinking through the privacy-privacy trade-offs embedded in the current legal approach.

Specifically, the third category outlined by Professor Solove—information dissemination to the public—is granted extensive protection under the current

[283] Solove, *supra* note 35, at 482 (introducing a new legal framework focused on the "specific activities that pose privacy problems"). This taxonomy has proven influential in the field of privacy law. *See* Angel & Calo, *supra* note 116, at 510 (describing Solove's scholarship, including his taxonomy, as having "shap[ed] the field of American privacy scholarship for decades"). It has also garnered critiques. *See, e.g.*, *id.* at 511 (setting forth reasons why "the long-dominant social-taxonomic approach to privacy and privacy law is no longer serving the field"); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142 (2011) (critiquing absence of "a limiting principle or rule of recognition" in taxonomical approach).

[284] *See* Pozen, *supra* note 34, at 229. Professor Solove's taxonomy has been criticized for failing to resolve these tensions. Angel & Calo, *supra* note 116, at 551-52; Pozen, *supra* note 34, at 227-28 ("[The] capaciousness [of Solove's taxonomy] exacerbates the dilemma of privacy-privacy tradeoffs. The more sorts of privacy claims that there are, the greater the risk that there will be conflicts among them."). But it does provide a vehicle for identifying where such tensions exist.

[285] Solove, *supra* note 35, at 491.

[286] *Id.* at 505-06.

[287] *Id.* at 525.

[288] *Id.* at 552-53 (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890)).

[289] *Id.* at 491 ("Invasion, unlike the other groupings, need not involve personal information . . . ."). Of course, police searches can intrude on one's solitude. But this Article is more focused on the data collection implications of government surveillance, rather than the infringement on one's solitude imposed by the physical intrusion of police. *See id.* at 550.

legal approach,[290] at least for certain groups.[291] Law enforcement agencies have myriad statutory and constitutional tools at their disposal to prevent the public release of private information contained in police records.[292] And judges have bolstered these secrecy powers by developing doctrines that further privilege the government in information disputes, as well as by citing the increased accessibility of electronic information as a reason to be more cautious about disclosing records to the public.[293] Landmark FOIA decisions at the federal level have baked these considerations into the law's privacy exemption.[294]

In short, this category of privacy harms is taken seriously under the present construction of the law. These anti-disclosure provisions offer protection against the social consequences of information dissemination to the public. They minimize the risk that a neighbor, coworker, friend, or journalist will obtain sensitive information that was initially gathered by police about an individual. If someone calls 911 because their child is having a mental health crisis, for instance, the existing public records regime helps prevent that child's social circle from learning about the incident. If someone is a victim of a sexual crime, the current legal approach protects against that information being shared without their consent with the victim's coworkers, relatives, or neighbors.

Yet, the first two categories of privacy intrusions—information collection and processing—receive less protection under the current law.[295] When it comes to

[290] Professor Solove described this category as encompassing both "disclosure" and "increased accessibility . . . of information." *Id.* at 491.

[291] Many categories of criminal justice records are not granted protection against public dissemination. *See* Scott Skinner-Thompson, *Agonistic Privacy & Equitable Democracy*, 131 YALE L.J.F. 454, 464 (2021), https://www.yalelawjournal.org/forum/agonistic-privacy-equitable-democracy [https://perma.cc/HU3W-8SC6] ("With the proliferation of digitized criminal records and online mugshot databases, once a person is criminalized, they are always criminalized." (footnotes omitted)).

[292] For a summary of the many ways that police are granted secrecy tools under federal and state public records statutes, see Koningisor, *supra* note 19, at 637-50.

[293] *See, e.g.*, Detroit Free Press Inc. v. U.S. DOJ, 829 F.3d 478, 482 (6th Cir. 2016) ("Today, an idle internet search reveals the same booking photo that once would have required a trip to the local library's microfiche collection.").

[294] *See, e.g.*, U.S. DOJ v. Reps. Comm. for Freedom of Press, 489 U.S. 749, 771, 780 (1989) (extending FOIA Exemption 7(C) to shield FBI rap sheets even though much of the information is already publicly available because "in today's society the computer can accumulate and store information that would otherwise have surely been forgotten"). *But see* Solove, *supra* note 35, at 509 ("*Reporters Committee* is one of the rare instances where the law has recognized that aggregation can make a material difference in what is known about an individual.").

[295] This emphasis on ex post protection against data sharing at the expense of ex ante protection against data collection can also be seen elsewhere in the privacy law regime. *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 600-05 (1977) (emphasizing privacy interest in nondisclosure of medical records but minimizing privacy interest in protecting against data collection in first instance); *see also* Gamal, *supra* note 15, at 1327-39 (describing privacy

information collecting, virtually every sectoral privacy statute—including those that protect medical information, children's data online, and so on—carves out an exception for law enforcement agencies.[296] And when it comes to government searches and surveillance, the Court has watered down constitutional protections in recent years.[297] It has also diminished constitutional protections against persistent police surveillance in public spaces.[298] Police today have ample information-gathering powers, with limited restraints. They have broad authority to create government data in the first place.[299]

Professor Solove's second category of privacy intrusions—information processing—also receives lesser protections under the current approach.[300] Once law enforcement agencies have accessed private information, there are few restrictions on the further combination of these disparate sources of data. To the contrary, the existing legal regime tends to promote data sharing and aggregation.[301] Information gathered by one law enforcement agency routinely ends up in law enforcement databases like Fusion Centers or federal and state crime information centers, where it is then combined and shared widely among other local, state, and federal law enforcement actors.[302]

There are also few barriers against the further dissemination or secondary use of information gathered by police and later shared with non-law-enforcement

law's emphasis on nondisclosure over protection against data gathering); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 964 (2017) (criticizing Fair Information Practices as "formalistic exercises designed to extract consent and use the gift of control to saddle the data subject with the risk of loss for data misuse").

[296] *See* Murphy, *supra* note 12, at 487.

[297] *See, e.g.*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1166 (2021) (describing limitations of Fourth Amendment when it comes to protecting against facial recognition technologies); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 184-87 (2016) (arguing increased knowledge about government surveillance activities can reduce scope of Fourth Amendment protections).

[298] *See, e.g.*, United States v. Diaz-Castaneda, 494 F.3d 1146, 1150 (9th Cir. 2007) (listing cases across different jurisdictions finding license plate data collection is not a "search" under the Fourth Amendment); *see also* I. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 964-77 (2013) (describing how Fourth Amendment doctrine fails to offer meaningful protection against public surveillance).

[299] *See* LOWRY PRESSLY, THE RIGHT TO OBLIVION: PRIVACY AND THE GOOD LIFE 4-6 (2024) (critiquing contemporary approach to privacy for emphasizing protection of existing data rather than opposing creation of data).

[300] Solove, *supra* note 35, at 519 (noting courts are generally "reluctant to find harm simply from the insecure storage of information" without showing of "overt harm" stemming from that improper storage).

[301] *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1442-44 (2011) (describing increase in domestic intelligence information-sharing in wake of 9/11).

[302] *See National Network of Fusion Centers Fact Sheet*, HOMELAND SEC., https://www.dhs.gov/national-network-fusion-centers-fact-sheet (last visited Jan. 6, 2025).

government actors.[303] Again, to the contrary, data collected by law enforcement agencies is routinely repurposed to serve other ends.[304] And vice versa—information gathered for non-law-enforcement purposes is regularly coopted by law enforcement agencies to serve distinct goals.[305] The law explicitly permits such secondary uses when it comes to police-gathered data.[306] In sum, the current legal approach protects against the harms of public disclosure at the expense of data collection and processing harms.

This trade-off raises several concerns. First, it creates what Professor Pozen has referred to as a "dynamic tradeoff," or a privacy shift "across time periods."[307] The present legal regime privileges privacy intrusions that occur later in the information processing regime at the expense of those that occurred earlier. Yet, this initial privacy intrusion may be distinctly harmful—it may be the first time someone has surrendered control over a particular piece of information.[308] It may also create information and data that otherwise might not have existed.[309] Such a process will be especially invasive if an individual is forced to make these disclosures against their will.[310]

Second, the current legal framework privileges privacy harms imposed by certain actors over others—or a "directional tradeoff."[311] The privacy harms

[303] *See, e.g.*, FBI v. Abramson, 456 U.S. 615, 631-32 (1982) (holding information gathered for law enforcement purposes retains Exemption 7 protection under FOIA even when included in records compiled for non-law-enforcement purposes).

[304] There are myriad examples of this. *See, e.g.*, Solove, *supra* note 30, at 1138-39 (discussing secondary uses of "federal, state, and local public records," including trading among private companies).

[305] *See, e.g.*, Solove, *supra* note 35, at 520 (providing example of federal government using databases from private businesses to detect fraudulent behavior).

[306] *See, e.g.*, Driver's Privacy Protection Act of 1994, 18 U.S.C § 2721(b)(1) (carving law enforcement and government agencies out of protections against secondary use of personal information).

[307] Pozen, *supra* note 34, at 229.

[308] There is no clear consensus for how to weigh and rank such privacy-privacy tradeoffs. *See id.* But scholars have suggested different approaches. *See, e.g.*, SCOTT SKINNER-THOMPSON, *Outing Privacy as Anti-Subordination*, *in* PRIVACY AT THE MARGINS 139, 158-79 (2020) (arguing for categorical privacy approach that would privilege intimate and political information over others, due to their direct material consequences); Angel & Calo, *supra* note 116, at 556 (focusing on "precise work privacy is doing within contemporary information problems" as way to mediate against such competing interests).

[309] *See* Pressly, *supra* note 299, at 6 (critiquing assumption that "information has a natural existence in human affairs, and that there are no aspects of human life which cannot be translated somehow into data").

[310] This is why consent has played such a central (if controversial) role in the construction of privacy law. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1462-63 (2019).

[311] Pozen, *supra* note 34, at 229 ("An e-reader such as Amazon's Kindle prevents my fellow riders on the subway from seeing what I am reading, but it tells Amazon in great detail about what I am reading, including how many seconds I have spent on each page.").

imposed by private actors armed with public data are accounted for under the current approach. Yet when police gather and maintain data, they do so with the full force of the state behind them. Information in law enforcement hands can open someone up to criminal sanctions and other penalties imposed by the state. Certain types of harms—for example, the risk of embarrassment from disclosure to friends or neighbors—may be reduced under the current approach. But other harms, such as the risk of criminal prosecution or police violence, are increased.[312]

Third, these privacy-privacy trade-offs allow the government to engage in a kind of "privacywashing"[313] of surveillance intrusions. Law enforcement agencies promise to keep private information secure in exchange for privileged access to private data.[314] But they often fail to uphold their end of the bargain. Government data breaches are routine.[315] Police officers abuse their access powers to obtain data for personal reasons or to sell information for financial gain.[316] And massive intergovernmental data pools amplify access and magnify the risk for abuse.[317] The promise of data protection is often a false one, and yet it is used to sell the public on ever-increasing powers of police surveillance and data aggregation.

In sum, the current regime protects against ex post dissemination to the public of private facts gathered by government. But in doing so, it facilitates other types of privacy harms. It underprotects against the intrusions imposed by police information gathering. And it undervalues the costs of data aggregation and processing harms.

---

[312] *See* Skinner-Thompson, *supra* note 291, at 459 (arguing state-sponsored surveillance leads members of marginalized communities to withdraw from "public square" to avoid "state-sanctioned physical violence").

[313] Rory Mir & Cory Doctorow, *Facebook's Attack on Research Is Everyone's Problem*, EFF (Aug. 12, 2021), https://www.eff.org/deeplinks/2021/08/facebooks-attack-research-everyones-problem [https://perma.cc/G6ZQ-2VKT].

[314] *Compare* Murphy, *supra* note 12, at 504 (describing how law enforcement agencies "regularly and routinely weigh in to address the impact that statutory protections will have on their interests," and "help shape or guide the scope of the inevitable law enforcement exemption" in privacy statutes), *with* 5 U.S.C. § 552(b)(7)(C) (establishing heightened privacy protections for law enforcement records).

[315] *See Top 10 Biggest Government Data Breaches of All Time in the U.S.*, DIGITAL GUARDIAN (Apr. 10, 2017), https://www.digitalguardian.com/blog/top-10-biggest-government-data-breaches-all-time-us [https://perma.cc/T37Q-FA67].

[316] *See* Sadie Gurman & Eric Tucker, *Across US, Police Officers Abuse Confidential Databases*, AP NEWS (Sept. 28, 2016, 12:28 AM), https://apnews.com/general-news-699236946e3140659fff8a2362e16f43 (describing instances of police officers spying on co-workers and selling information to private investigators).

[317] *See* Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007, 1010 (2022) ("[O]ne government's flawed data collection can be easily amplified by data exchanges—as when a city that disproportionately polices a minority population infuses its biased data into a cross-governmental database.").

B. *Distributive Harms*

The current privacy law regime also embodies a set of normative choices about whose privacy matters and how these privacy privileges are dispensed. Such protections are not distributed equally; rather, they favor the interests of the powerful at the expense of marginalized communities.[318] In this way, police privacy cooption plugs into a broader discussion about the subordinating effects of privacy law.[319]

Privacy interests that benefit police are often granted substantial weight under the current public records regime. Some states provide law enforcement officers with greater personnel file protection than other government employees, for example.[320] But even when police are granted equal privacy protections on the face of the law, their interests often receive outsized consideration in practice.

[318] There is a rich body of literature exploring how oppressed communities receive reduced privacy protections. *See, e.g.*, SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 15 (2018) (demonstrating race and sex discrimination embedded within search engine algorithms); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J.F. 907, 910 (2022), https://www.yalelawjournal.org/pdf/F7.AllenFinalDraftWEB_6f26iyu6.pdf [https://perma.cc/G3RF-X9FM] (describing "compounding vulnerabilities" that Black Americans face when it comes to data privacy intrusions); Arnett, *supra* note 31, at 642 (describing privacy harms imposed by surveillance in criminal justice system); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 693 (2016) (describing how data mining can replicate existing patterns of societal bias and discrimination); Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J.L. & GENDER 113, 116-17 (2011) (describing how public assistance for state prenatal care involves data gathering that imposes significant privacy harms); Bridges, *supra* note 31, at 116-17 (exploring poverty disparities in how privacy protections are dispensed); Kimberlé W. Crenshaw, *From Private Violence to Mass Incarceration: Thinking Intersectionally About Women, Race, and Social Control*, 59 UCLA L. REV. 1418, 1427 (2012) (describing the "many ways that surveillance and punishment are intersectionally scripted, including the ways in which race, gender, or class hierarchies structure the backdrop against which punitive policies interact"); Murphy, *supra* note 12, at 508-14 (describing ways federal privacy statutes fail to protect privacy of poor people); Skinner-Thompson, *supra* note 308 (examining the many ways that privacy law under-protects marginalized communities). A closely related concept is that of "differentiated privacy harms," or the idea that privacy harms impact different groups in different ways. *See* Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1403 (2012) (illustrating how low-wage workers are often subjected to more invasive surveillance such as drug tests). Scholars have also written about the tension between privacy and equality, especially in the context of women and LGBT communities. *See, e.g.*, Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1875 (2019) (describing how insufficient sexual privacy protections harm women and other marginalized communities); Kenji Yoshino, *Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of "Don't Ask, Don't Tell,"* 108 YALE L.J. 485, 554 (1998) (arguing privacy law imposes specific harms on LGBT community).

[319] *See* Allen, *supra* note 318.

[320] *See supra* note 195 and accompanying text.

For example, courts may initially deny a privacy claim when a citizen brings it, and then reverse the decision and extend protection once law enforcement interests are involved.[321] Police departments, too, withhold information about police officers that they routinely disclose about other citizens,[322] or withhold information from an adverse party while simultaneously releasing that same information to officers within the department.[323]

The privacy interests of the wealthy and powerful are often granted substantial protection as well, especially for groups politically aligned with law enforcement interests. The National Rifle Association ("NRA"), for example, provides broad political and financial support to law enforcement agencies. These links are deep and entrenched; the NRA has "advocated on behalf of police as professional gun wielders since the early twentieth century."[324] Gun owners are also wealthier, on average, than those who do not own guns.[325]

Gun permit data, in turn, receives extensive protection against disclosure. More than two-thirds of states have enacted explicit protections for gun permit application data.[326] And at the federal level, Congress has enacted a law prohibiting the creation of a national weapons database.[327] The NRA was involved with drafting and lobbying for these provisions.[328] Additionally, many

[321] *See, e.g.*, Detroit Free Press Inc. v. U.S. DOJ, 829 F.3d 478, 480 (6th Cir. 2016) (reversing panel decision and finding that there is privacy interest in mugshots in context of request for mugshots of arrested police officers).

[322] *See, e.g.*, Trevor Dunnell, *Violation of Public Record Law: New Bern Police Department Withholding Records*, SHELBY STAR, https://www.shelbystar.com/story/news/2021/09/29/public-records-request-denied-city-new-bern-against-law-police-department-salary/5884256001/ [https://perma.cc/4JLS-TQZM] (last updated Oct. 2, 2021, 8:51 AM) (describing how city released names of all government employees except for police officers); Jan Ransom, *Police Abuse Exemption in Public-Records Law, Reform Panel Is Told*, BOS. GLOBE (May 3, 2017, 8:38 PM), https://www.bostonglobe.com/metro/2017/05/03/police-abuse-exemption-public-records-law-reform-panel-told/iT8Fp9BovWqPnz7bHla72H/story.html (describing how police withhold names of police officers or judges accused of crimes while routinely revealing names of citizens accused of similar crimes).

[323] *See* discussion *supra* note 177 and accompanying text.

[324] JENNIFER CARLSON, POLICING THE SECOND AMENDMENT: GUNS, LAW ENFORCEMENT, AND THE POLITICS OF RACE 8 (2020)

[325] *See* Jay Willis, *Owning a Gun in America Is a Luxury*, GQ (Apr. 30, 2018), https://www.gq.com/story/gun-ownership-cost [https://perma.cc/5EBA-ZTS3].

[326] *See* Koningisor, *supra* note 19, at 645 n.177 (listing exemptions for gun permit application data).

[327] Murphy, *supra* note 12, at 514.

[328] Joel Achenbach, Scott Higham & Sari Horwitz, *How NRA's True Believers Converted a Marksmanship Group into a Mighty Gun Lobby*, WASH. POST (Jan. 12, 2013), https://www.washingtonpost.com/politics/how-nras-true-believers-converted-a-marksmanship-group-into-a-mighty-gun-lobby/2013/01/12/51c62288-59b9-11e2-88d0-c4cf65c3ad15_story.html.

state-level protections were passed after coordinated political efforts by the NRA.[329]

Data gathered from a broader cross section of the public also receives heightened protection. Examples include amendments to public records statutes to explicitly exclude categories like automated license plate data.[330] They also include enhanced protections granted to data gathered from more diverse socioeconomic classes—for example, social security data or tax filings, which receive substantial protection.[331] In contrast, data collected from poorer groups, such as welfare recipients, tends to be more publicly accessible.[332] The end result is that surveillance that captures wealthier populations receives greater protection against ex post dissemination harms.[333]

In contrast, those accused or convicted of crimes receive reduced protection. Virtually every state discloses arrest record information under its public records statute, for instance.[334] Many states also disclose mugshot photos.[335] Various other categories of criminal information are made readily available to the public as well, including compilations of criminal history.[336] The impact of these laws is significant: Roughly a third of the adult population in the United States has a record on file with criminal justice agencies.[337] And because of the staggering

[329] *See* Koningisor, *supra* note 130, at 1506-07.

[330] *See, e.g.*, GA. CODE ANN. § 35-1-22(f) (2025); UTAH CODE ANN. § 63G-2-305(63) (LexisNexis 2024).

[331] Murphy, *supra* note 12, at 512.

[332] *Id.*; *see also* JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 35 (2001) (describing rise of "digital poorhouse" in which poor people are forced to surrender intimate data in exchange for government assistance).

[333] At the same time, participants in government assistance programs are also compelled to surrender more sensitive data to the government ex ante. *See, e.g.*, Bridges, *supra* note 318, at 116-17 (describing sensitive data collected about pregnant people who receive government assistance); Gamal, *supra* note 15, at 1347 (describing reduced privacy protections for educational records of students who receive government assistance). The government both captures more private information from these groups and provides reduced protections for its further dissemination.

[334] *See* State Law Comparisons Spreadsheet, *supra* note 44; *see also* Denver Policemen's Protective Ass'n v. Lichtenstein, 660 F.2d 432, 436-37 (10th Cir. 1981) (noting "iron[y]" of police association's position that "its right to privacy is the same as a citizen's" while also conceding that citizens' rap sheets are "routinely discoverable").

[335] *See* State Law Comparisons Spreadsheet, *supra* note 44.

[336] *See, e.g.*, COLO. REV. STAT. § 24-72-303(1) (2025) (opening records of criminal justice agencies taking official actions); ME. STAT. tit. 16, § 703(2)-(3) (2025) (providing public access to conviction data); MONT. CODE ANN. § 44-5-302 (West 2025) (permitting public access to criminal history data); *see also* State Law Comparisons Spreadsheet, *supra* note 44 (providing comparisons of state treatment of different categories of police records); ARIZ. CONST. art. 4.2, § 22 (requiring disclosure of criminal records of juveniles and providing exceptions only for "the protection of the privacy of innocent victims of crime" or finding of clear public interest in confidentiality).

[337] Brayne, *supra* note 113, at 825.

racial and socioeconomic disparities in criminal justice prosecutions, those with police records are much more likely to be poor individuals and individuals of color.[338]

Further, similar categories of police records are not always made available to the public. Arguments that prove persuasive when applied to police officers under investigation—for example, concerns about due process and fairness when disclosing unsubstantiated complaints against police—are not given equal weight when applied to the public at large.[339] Many of the same states that disclose mugshot photos or arrest records, for instance, also withhold police photos or unproven complaints against police.[340] Police also selectively enforce certain privacy provisions. For instance, they will invoke automatic sealing statutes to shield body camera footage from investigators but permit access to the very officers who are being investigated.[341]

Such double standards are pervasive in both law and practice, and they disproportionately affect individuals from oppressed communities who are at greater risk of becoming enmeshed in the criminal justice system in the first place.[342] Professor Jack Balkin likens such discrepant privacy rules to "a great two-way mirror in which ordinary people's lives are increasingly transparent to powerful public and private entities that are not transparent to the people they view."[343] Privacy cooption adds an additional layer to this dynamic. Under the current privacy law regime, individuals are not necessarily stripped of their

[338] *See, e.g.*, PEW, RACIAL DISPARITIES PERSIST IN MANY U.S. JAILS 2 (2023), https://www.pewtrusts.org/-/media/assets/2023/05/racial_disparities_persist_in_many_us_jails_brief_digital.pdf [https://perma.cc/PZ8K-E7XN] ("Black people were admitted to jail at more than four times the rate of White people and stayed in jail for 12 more days on average across the 595-jail sample . . . ."); ADAM LOONEY & NICHOLAS TURNER, BROOKINGS INST., WORK AND OPPORTUNITY BEFORE AND AFTER INCARCERATION 12 (2018), https://www.brookings.edu/wp-content/uploads/2018/03/es_20180314_looneyincarceration_final.pdf [https://perma.cc/3PHL-NX5Y] (finding boys who grew up in poorest families are forty times more likely to end up in prison compared to boys who grew up in richest families).

[339] Professor Kate Levine argues that the best way to resolve these discrepancies is not to diminish privacy protections for police, but instead to ramp up privacy protections for everyone to the standards enjoyed by police. *See* Levine, *supra* note 27, at 847-48.

[340] *Compare, e.g.*, FLA. STAT. ANN. § 119.071(4)(d)(2) (West 2024) (shielding "photographs of active or former sworn law enforcement personnel"), *with id.* § 119.071(2)(c)(1), *and id.* § 119.07(1) (providing that all nonexempt records, including police records and mugshots, are subject to disclosure unless exempt as criminal intelligence information).

[341] Memorandum from Carayannis, *supra* note 150, at 3 (reporting NYPD has a blanket policy of denying requests for footage by investigators).

[342] *See, e.g.*, MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS 16 (2010) ("[M]ore than half of the young [B]lack men in many large American cities are currently under the control of the criminal justice system (or saddled with criminal records) . . . .").

[343] Jack M. Balkin, *Room for Maneuver: Julie Cohen's Theory of Freedom in the Information State*, 6 JERUSALEM REV. LEGAL STUD. 79, 95 (2012).

privacy rights altogether. Rather, their privacy rights may be nominally preserved but asserted selectively by police when doing so advances law enforcement interests.

Conversely, privacy protections are much more likely to operate as a barrier to evidentiary access for those accused of a crime. Many privacy statutes have exemptions that permit law enforcement agencies to access protected material but contain no similar access provision for criminal defendants.[344] Similar access inequities exist under transparency statutes, too. Under FOIA, privacy interests are balanced against the public interest in disclosure.[345] But the federal courts have held that the public interest only extends to materials that "shed[] light on an agency's performance of its statutory duties."[346] They have repeatedly held that defendants' need to obtain evidentiary records does not qualify under this standard, even though individual cases can shed light on broader systemic problems within an agency. Such a justification, they have reasoned, does not constitute a "public interest" that is cognizable under the statute.[347]

These statutory inequities are exacerbated by constitutional disparities. The Fourth Amendment protects against police intrusion onto private property. But poor people are forced into public spaces where they have reduced constitutional protections against police searches and seizures.[348] Centuries of discrimination and oppression have led to profound and persistent racial disparities in wealth in this country.[349] The end result is impoverished constitutional privacy protections against information collection for poor communities and communities of color.[350] At the same time, there are also reduced statutory barriers to prevent police from releasing this information under public records laws.[351]

Such statutory protections against the disclosure of surveillance data can advance important distributive and equity goals.[352] But they also make it more difficult for these communities to access information that would help them

[344] Wexler, *supra* note 15, at 215.

[345] 5 U.S.C. § 552(b)(7)(C).

[346] *See* U.S. DOJ v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 773 (1989).

[347] U.S. DOJ, GUIDE TO THE FREEDOM OF INFORMATION ACT: EXEMPTION 7(C), at 23 (2025), https://www.justice.gov/oip/page/file/1206756/dl [https://perma.cc/8XE3-XL3D] ("[C]ourts have rarely recognized any public interest in disclosure of information sought to assist someone in challenging their conviction."). One exception is for records relating to death row inmates. *See* Roth v. U.S. DOJ, 642 F.3d 1161, 1181-82 (D.C. Cir. 2011).

[348] *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 124 (2000) (holding evading law enforcement in high crime area is sufficient to establish reasonable suspicion); *see also* Stuntz, *supra* note 18, at 1266; SKINNER-THOMPSON, *supra* note 308, at 15; discussion *supra* note 318 (listing scholars who address inequality in privacy law regime).

[349] *See* ALEXANDER, *supra* note 342, at 185.

[350] *See* Stuntz, *supra* note 18, at 1266 ("Fourth Amendment law makes wealthier suspects better off . . . and may make poorer suspects worse off."); *see also supra* note 332 and accompanying text.

[351] *See supra* notes 340-41 and accompanying text.

[352] *See supra* notes 78-82 and accompanying text.

oppose such surveillance systems in the first place.[353] And they can impose barriers to punishing police wrongdoing after the fact.[354] The history of racialized surveillance in this country stretches back before the founding.[355] And these inequities persist today. Black communities are subjected to both over- and under-policing,[356] as well as much greater levels of police surveillance.[357] The federal government also gathers both more and more intrusive data about poor individuals and families—for example, requiring welfare recipients to provide detailed information about the paternity of children who receive benefits.[358] Such data is almost always accessible to police.[359]

As a result, the current regime forces those communities subjected to extensive police surveillance to choose between two types of privacy harms. Reducing back-end privacy protections would expose these same communities to even greater public scrutiny. But such protections also function as a barrier to understanding how this surveillance is being conducted. This forces poor communities, Black communities, and other communities subjected to persistent police surveillance into a difficult choice: either surrender additional privacy by opening police records to public view; or maintain these ex post privacy protections at the risk of not learning about such surveillance in the first place.[360]

[353] They also make it more difficult for the accused to obtain evidence that might be relevant to mount their defense. *See* Wexler, *supra* note 15, at 229 (contrasting information privacy statutes' "express textual exceptions that authorize disclosures to law enforcement" with their silence regarding disclosures to criminal defendants).

[354] *See, e.g.*, JOANNA SCHWARZ, SHIELDED: HOW THE POLICE BECAME UNTOUCHABLE 226 (2023) (describing how information barriers, including barriers to obtaining names of specific police officers, stifle Section 1983 claims against law enforcement agencies).

[355] *See generally* MARY FRANCES BERRY, BLACK RESISTANCE/WHITE LAW (1995) (describing racialized surveillance practices stretching back to the founding); Browne, *supra* note 273 (examining this history from sociological perspective).

[356] *See* Devon W. Carbado, *From Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence*, 105 CALIF. L. REV. 125, 127-29 (2017) (describing problem of "racially disproportionate policing").

[357] *See id.*; ALEXANDER, *supra* note 342, at 94-96.

[358] *See* Murphy, *supra* note 12, at 509; Gamal, *supra* note 15, at 1347 (describing reduced privacy protections for "school welfare" educational records).

[359] Murphy, *supra* note 12, at 510 (describing how police "mine welfare and housing rolls to apprehend persons with outstanding warrants").

[360] The stakes of this choice are high: The harms are not limited to privacy intrusions alone. There is a direct link between excessive police surveillance and infliction of police violence. *See* Carbado, *supra* note 356, at 128 (describing "the significant 'circuits of violence' through which the ordinary (African Americans' vulnerability to ongoing police surveillance and contact) becomes the extraordinary (serious bodily injury and death)"). Further, increasing access to information about police surveillance alone will not be sufficient to meaningfully contest or end such surveillance. *See* Ngozi Okidegbe, *The Democratizing Potential of Algorithms?*, 53 CONN. L. REV. 739, 746 (2022) ("[T]ransparency on its own is inattentive to the 'layers of democratic exclusion' that reinforce the political powerlessness experienced by

C. *Democracy Harms*

Privacy has myriad democratic benefits. It allows citizens the space needed to think, write, develop ideas, and organize.[361] It prevents the chilling of private speech and thought.[362] It permits people to form their own opinions, views, and conceptions of selfhood, free from undue influence.[363] It protects against conformity and heterogeneity.[364] It provides "room to breathe" for "novel but unpopular ideas."[365] And so on.

Yet privacy protections also impose democratic costs. In the context of police records, they do so by shielding information about law enforcement agencies from the public.[366] This risk is exacerbated by current public records laws, which require the government to invoke privacy interests on citizens' behalf.[367] And when they do so, there are a complicated set of incentives at play. The government is often the entity that gathered the private information in the first place.[368] And in the context of policing, the victim of police violence may be the

those most harmed by the system, who are thus unable to change the system or dismantle and reconstitute it."). Yet obtaining information about policing can be a useful antecedent to more radical change. Records documenting sources of police funding, for example, can be useful in supporting efforts to defund the police. Information about 911 calls can be useful in constructing a government emergency response apparatus that prioritizes "non-carceral and health-based responses." *See Policy*, BLACK LIVES MATTER, https://impact.blacklivesmatter.com/policy/ [https://perma.cc/72G2-MB5Y] (last visited Apr. 10, 2025).

[361] *See* Berger v. New York, 388 U.S. 41, 125 (1967) (White, J., dissenting) ("In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively.").

[362] *See* Cohen, *supra* note 278, at 1912 ("A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy.").

[363] *See id.* at 1905 ("Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable.").

[364] *See* Scott Skinner-Thompson, *supra* note 291, at 455 (describing societal-level democratic harms imposed by insufficient privacy protections).

[365] Richards, *supra* note 275, at 403.

[366] *See* discussion *supra* Section III.B (discussing various informational barriers to disclosure of police information). A closely related line of cases and body of literature critiques privacy protections on free speech grounds. *See, e.g.*, Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989) (striking down privacy statute on First Amendment grounds); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000) (arguing that "broader information privacy rules are not easily defensible under existing free speech law").

[367] *See, e.g.*, 5 U.S.C. § 552(b)(6) (outlining conditions under which government may invoke privacy interests of individuals as reason for nondisclosure under FOIA).

[368] There are some exceptions—for instance, when the government purchases or compels private data gathered by a nonstate actor. *See, e.g.*, Matthew Tokson, *Government Purchases of Private Data*, 59 WAKE FOREST L. REV. 269, 283-87 (2024).

very person whose privacy interests are being invoked.[369] This leads to the persistent risk that these privacy exemptions will be coopted for anti-accountability ends.

Such information barriers introduce a cascading set of democratic harms. Privacy protections can impede the process of democratic self-governance. Under a Meiklejohnian view of the First Amendment, public access to government information is a prerequisite to fostering the deliberative debate that gives rise to democratic self-government.[370] Such concerns motivate doctrines like the First Amendment right of access.[371] Similar justifications underlie statutory rights of access as well.[372] But the powerful privacy protections extended to law enforcement agencies inhibit this democratic feedback loop.[373] They make it more difficult for the public to understand what police are up to.[374] Even when there are legitimate privacy interests at stake in police records, police secrecy still impedes meaningful public oversight. Ramping up privacy in police records reduces the public's ability to monitor police under the current

[369] *See supra* Section II.B.1.

[370] *See* Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 257 ("Public discussions of public issues, together with the spreading of information and opinion bearing on those issues, must have a freedom unabridged by our agents.").

[371] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 587 (1980) (Brennan, J., concurring) ("Implicit in this structural role [of the First Amendment] is not only 'the principle that debate on public issues should be uninhibited, robust, and wide-open,' but also the antecedent assumption that valuable public debate—as well as other civic behavior—must be informed." (citation omitted)).

[372] *See, e.g.*, MICH. COMP. LAWS ANN. § 15.231 (West 2025) ("The people shall be informed so that they may fully participate in the democratic process."); N.Y. PUB. OFF. LAW § 84 (McKinney 2025) ("The legislature hereby finds that a free society is maintained when government is responsive and responsible to the public, and when the public is aware of governmental actions.").

[373] Not all scholars agree that increased transparency always promotes of democratic ideals and values. There is an important body of scholarship critiquing the democratic value of transparency. *See, e.g.*, Michael Schudson, *The Shortcomings of Transparency for Democracy*, 64 AM. BEHAV. SCIENTIST 1670, 1675 (2020) (describing flawed premises that undergird transparency laws); Brigham Daniels, Mark Buntaine & Tanner Bangerter, *Testing Transparency*, 114 NW. U. L. REV. 1263, 1273-74 (2020) (finding reduced public participation in government meetings as administrative transparency increases). These critiques are often persuasive. And in the specific context of policing, transparency alone is a necessary but not sufficient condition for securing meaningful democratic oversight and accountability. *See* Levine, *supra* note 27, at 845; Okidegbe, *supra* note 360, at 746. The public must be vested with meaningful decision-making power. *See* Jocelyn Simonson, *Police Reform Through a Power Lens*, 130 YALE L.J. 778, 786-87 (2021) (describing proposals to "create new forms of governance arrangements that shift power over policing to those who have historically been the targets of policing").

[374] This point is embedded within the balancing test contained in Exemption 7 and many other state privacy exemptions from public records disclosures. *See* 5 U.S.C. § 552(b)(7).

transparency law regime. This is not a new insight.[375] But the lens of privacy cooption helps to conceptualize a fuller set of costs.

The clearest category of democratic harm includes police privacy assertions that are wholly pretextual. When there are no legitimate privacy interests at stake, these democratic costs are incurred without any meaningful corresponding privacy benefits. Examples include claiming privacy exemptions to withhold even anonymized or aggregated data.[376] They also include police officials admitting behind closed doors that they had falsely claimed privacy as a mechanism to forestall public scrutiny.[377] Police secrecy in these instances acts as an oversight cost without providing legitimate privacy benefits on the other side of the ledger.

A related set of democratic harms are introduced when privacy carveouts from public oversight become so broad that they essentially swallow the rule. The dramatic expansion in recent years of the amount and type of data collected by law enforcement agencies heightens this risk. Technological advancements have allowed police unprecedented access to massive amounts of citizen data, which is then aggregated, analyzed, and put to myriad other secondary uses.[378] The scope of information gathered is now so broad that citizen privacy interests can be invoked to shield huge swaths of police activity from public view. Such privacy claims are not necessarily pretextual. There may be legitimate privacy interests at stake. But they nonetheless impose substantial impediments to democratic oversight. At the extreme end, privacy concerns can be invoked to shield almost any facet of police activity from public view.

Again, consider the example of automated license plate data.[379] Shielding this data on privacy grounds makes intuitive sense. Such information might reveal private medical information, such as a visit to an abortion clinic, or personal information, like a new or illicit romantic partner.[380] Yet such information barriers also make it more difficult for the public to understand how these surveillance programs work—how much data is collected, how long it is stored,

---

[375] *See* discussion *supra* note 27 and accompanying text; *see also* ALAN WESTIN, PRIVACY AND FREEDOM 25 (1967) ("An overly strict cloak of privacy for governmental affairs can cover manipulation of the public, misuse of office, and aggrandizement of power by government agencies."); David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 286 (2010) ("Many of the modern era's most important political thinkers . . . and virtually all of the normative schools of democratic theory—from contractarians, to deliberativists, to libertarians, to republicans—have viewed transparency as a critical component of popular legitimacy and moral government.").

[376] *See supra* note 194 and accompanying text.

[377] *See supra* notes 9-11 and accompanying text.

[378] *See generally* Ferguson, *supra* note 31 (examining how predictive analytics, social network theory, and data-mining impact policing).

[379] For a summary of the technology, see *Automated License Plate Readers*, EFF, https://www.eff.org/pages/automated-license-plate-readers-alpr# [https://perma.cc/YT9P-TKDH] (last visited Apr. 10, 2025).

[380] *Id.*

and how broadly it is shared.[381] This, in turn, impedes public efforts to contest or limit data collection before the police secure access.

The anti-accountability effects of privacy protections can also incentivize the police to expand their data-gathering efforts. This primacy on ex post protections against information disclosure to the broader public comes at the expense of ex ante restrictions on what data is collected in the first instance. Taken to its logical extreme, the anti-accountability benefits of privacy protections might operate as a strong incentive for the police to gather ever-more sensitive data. The more data collected, the more powerful the government's arguments become for acquiring these sweeping privacy protections. Mass data sweeps can be weaponized as a mechanism for escaping public scrutiny. Paradoxically, the greater the privacy intrusion by police, the stronger the police's argument against disclosing that intrusion to the public. The public then becomes limited in its ability to impose democratic sanctions for such intrusions or to implement ex ante checks against future abuses.

Expansive privacy protections for mass surveillance data also increase the risk of "deep secrets," or information that is so hidden that the public is not even aware of its existence.[382] If the public knows the police are capturing license plate data, for example, but it doesn't know where the cameras are located, this is a shallow secret. In contrast, if the public is unaware of the invention of a particular surveillance technology that is being used by police, that is a deep secret.[383]

As various legal and political science scholars have shown, deep secrets are especially harmful to the democratic process.[384] A shallow secret can be debated, even when the particulars remain unknown. A deep secret cannot. Deep secrecy robs the electorate of the opportunity to discuss, contest, and ultimately decide on a government's course of action. It disrupts the process of democratic consent. And it prevents the public from imposing democratic consequences on the government officials who engaged in activities that the electorate would oppose if they were made aware of them.[385]

The democratic harms of deep secrets are exacerbated in the context of policing.[386] Government secrecy amplifies the risk of government misconduct and abuses of power. But this risk is heightened when it comes to law

[381] *See, e.g.*, ACLU Found. of S. Cal. v. Superior Ct., 400 P.3d 432, 434 (2017) (describing Los Angeles Police Department's withholding of ALPR data on privacy grounds).

[382] *See* Pozen, *supra* note 375, at 260-61.

[383] *Id.* (noting deep secrets of the state are "things we do not know we do not know").

[384] *See, e.g.*, AMY GUTMANN & DENNIS THOMPSON, DEMOCRACY AND DISAGREEMENT 121 (1996); Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 509 (2019) ("[S]ecrecy undermines the accountability of police technologies to the public at large, limiting the ability of citizens to use the levers of democracy to control their law enforcement agencies."); Pozen, *supra* note 375, at 288-92.

[385] Pozen, *supra* note 375, at 289-90.

[386] Manes, *supra* note 384, at 560.

enforcement agencies, which already operate as "a uniquely frightening tool of official domination,"[387] and wield a domestic monopoly on state-sanctioned violence,[388] often without meaningful sanctions or oversight.[389] Further, police are already granted exceptional deference when it comes to informational control, both by judges and legislators.[390] Police are therefore uniquely susceptible to become abusers of power. Deep secrets exacerbate this risk by further insulating wrongdoing from exposure.[391] They entrench existing power imbalances between police and the citizenry.[392]

Finally, such privacy protections impose democratic chilling effects.[393] They help to obscure police activity, including the use of new surveillance technologies and mass surveillance efforts by police. This increases the public's confusion over whether surveillance is occurring.[394] And in response to this uncertainty, citizens may choose to self-censor much more of their behavior in response to the mere possibility that they are being watched.[395]

Moreover, the groups most likely to be surveilled are also the ones most likely to remove themselves from the public sphere altogether.[396] Here, the democratic and distributive harms begin to converge. Such exclusion means that the dissenting voices most critical to challenging the prevailing democratic consensus may be pushed out. And the democratic ramifications of this loss can be significant. This is true under a variety of democratic theories. Political theories that center the importance of democratic discussion to achieving

[387] DAVID ALAN SKLANSKY, DEMOCRACY AND THE POLICE 109 (2008).

[388] *See* Jacob D. Charles & Darrell A.H. Miller, *Violence and Nondelegation*, 135 HARV. L. REV. F. 463, 464 n.7 (2022), https://harvardlawreview.org/forum/vol-135/violence-and-nondelegation/ [https://perma.cc/VJX3-YZZJ] (describing this history).

[389] *See, e.g.*, CIV. RTS. DIV., U.S. DOJ, INVESTIGATION OF THE BALTIMORE CITY POLICE DEP'T 10 (2016) (describing lack of investigations or sanctions for alleged misconduct); *see also* Maria Ponomarenko, *Rethinking Police Rulemaking*, 114 NW. U. L. REV. 1, 9 n.33 (2019).

[390] *See* Koningisor, *supra* note 19, at 654-55.

[391] Pozen, *supra* note 375, at 288.

[392] SKLANSKY, *supra* note 387, at 109 (describing ways law enforcement agencies aggregate political power).

[393] Jeremy Bentham, *Panopticon*, *in* THE PANOPTICON WRITINGS 29, 45 (Miran Božovic ed., Verso 2011) (1787).

[394] Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 157 (2007) ("[E]ven if the information is never used at trial, uncertainty about the government's intentions may still deter First Amendment activities.").

[395] *See* Solove, *supra* note 35, at 495 ("[T]here can be an even greater chilling effect when people are generally aware of the possibility of surveillance, but are never sure if they are being watched at any particular moment.").

[396] Skinner-Thompson, *supra* note 291, at 459.

consensus presuppose broad and equitable access to the public sphere.[397] And political theories that emphasize the role of dissent and contestation in the democratic system view outside or marginalized voices as especially crucial to the process of democratic formation.[398] Yet these are precisely the voices at risk of being driven out of the public sphere by pervasive police surveillance.[399] The exclusionary effects of police information gathering on the public debate impose democratic costs in this way as well.

Privacy scholars have made this point in the context of arguing in favor of greater ex ante protections against government surveillance.[400] Yet in order to contest such pervasive surveillance, the public must first know about it—not just the mere fact that it is happening, but also the specifics of where and how it is being conducted and who is sponsoring and funding it. Under the current police records regime, the privacy interests in the data collected by police can operate as a barrier to understanding and contesting such surveillance in the first place.

IV. THE FUTURE OF PRIVACY IN POLICE RECORDS

The current approach to establishing privacy protections in police records is flawed. But the solution is not to throw open police files and allow the public unfettered access. This would impose steep privacy costs. Instead, we should rethink the role of the police and the capacity of police to gather, aggregate, and disseminate private information in the first place. We should sequence reforms to ensure that data collection is reduced before any significant privacy protections are relinquished. And we should allocate decision-making power

[397] *See, e.g.*, JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE 85 (Thomas Burger with Frederick Lawrence trans., Mass. Inst. of Tech. 1989) ("A public sphere from which specific groups would be *eo ipso* excluded was less than merely incomplete; it was not a public sphere at all."); *see also* Skinner-Thompson, *supra* note 291, at 465-67 (describing democratic implications of protecting popular participation under various democratic theories).

[398] *See, e.g.*, Chantal Mouffe, *Deliberative Democracy or Democratic Pluralism?*, 77 SOC. RSCH. 745, 756 (1999) (asserting that "the prime task of democratic politics is not to eliminate passions nor to relegate them to the private sphere in order to render rational consensus possible, but to mobilise those passions towards the promotion of democratic designs"); Chantal Mouffe, *Artistic Activism and Agonistic Spaces*, ART & RSCH., Summer 2007, at 1, 4-5 (arguing that democratic formation requires making "visible what the dominant consensus tends to obscure and obliterate" and "giving a voice to all those who are silenced within the framework of the existing hegemony").

[399] *See* Chaz Arnett, *Black Lives Monitored*, 69 UCLA L. REV. 1384, 1396-1403 (2023) (describing police surveillance of Black Lives Matter and other protests).

[400] *See, e.g.*, Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) ("Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."); Skinner-Thompson, *supra* note 291, at 464-70; Schwartz, *supra* note 54, at 1613 (arguing "poor privacy standards in cyberspace" will "discourag[e] participation in deliberative democracy").

more broadly and equitably when it comes to balancing the inevitable trade-offs between privacy and accountability in the context of policing.

A. *Reducing Police Surveillance*

One approach to mitigating the harms of privacy cooption would be to reduce police powers of data collection in the first place. Shrinking the amount of private information collected ex ante will make it more difficult for police to invoke privacy concerns ex post as an anti-accountability shield. There are many reasons to minimize police data collection.[401] But the problem of privacy cooption should be included among them. The current records regime allows police to gather large volumes of citizen data and then use the public's own privacy interests as a shield against public scrutiny. It also forces the communities most affected by pervasive police surveillance to choose between the harms of public disclosure and the harms of government data collection and processing in the first place. Limiting the amount of information that police gather in the first instance would reduce the stakes of this choice.[402]

There are different ways to reduce police surveillance powers. One approach would be to shrink the role and responsibilities of police altogether. Calls to divert police resources into services focused on the economic, medical, and social needs of marginalized communities, especially Black communities, are rooted in opposition to centuries of police violence.[403] Yet such changes could also have secondary privacy benefits. Police today are called to intervene at some of the most sensitive and difficult times of people's lives—during mental health crises, following the death of a loved one, or during domestic disputes.[404] Transferring these responsibilities to social workers or other healthcare professionals could have myriad benefits, including reducing privacy-based

[401] These reasons have been persuasively articulated by many activists and scholars. *See, e.g.*, Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1106 (2020) (arguing that "race- and class-targeted policing . . . actively facilitates the continued underdevelopment and subordination of these neighborhoods"); Southerland, *supra* note 112, at 17-24 (describing how policing surveillance are "tools of racial control").

[402] Privacy scholars have critiqued Professor Solove's taxonomy because it embodies overlapping privacy intrusions without providing a mechanism for mediating between them. *See* Angel & Calo, *supra* note 116, at 552 ("The taxonomic approach is silent—even agnostic—as to these emerging conflicts."). Yet avoiding these conflicts altogether offers an alternative.

[403] *See, e.g.*, Mariame Kaba, *So You're Thinking About Becoming an Abolitionist*, MEDIUM, https://level.medium.com/so-youre-thinking-about-becoming-an-abolitionist-a436f8e31894 (last updated Oct. 30, 2020).

[404] *See* Amna A. Akbar, *An Abolitionist Horizon for (Police) Reform*, 108 CALIF. L. REV. 1781, 1821 (2020) ("Policing and imprisonment have become the state's responses to social problems like houselessness, mental health crises, drug use, and unemployment, from which the state has otherwise divested.").

harms.[405] Such changes could decrease police data collection and record creation when it comes to especially sensitive information.

Shrinking police funding could also limit the amount of data police are able to gather.[406] There would be fewer resources available to engage in programmatic surveillance efforts. Divesting from police and reining in police budgets would likely limit the acquisition of costly new surveillance devices.[407] Data storage and management is expensive, and siphoning off police funds would likely operate as a natural barrier to the long-term or even indefinite maintenance of public data as well.[408]

Empowering groups that monitor police externally, without proceeding through formal transparency law mechanisms, could also reduce police privacy harms. Groups engaged in copwatching, court monitoring, ICE watching, and other similar efforts eschew formalized legal mechanisms for obtaining government information and instead create their own bodies of information and knowledge.[409] They write their own reports about police violence to contest the official police narrative.[410] And they gather their own criminal justice statistics—ones focused on holding judges and other criminal justice actors

[405] *Id.* at 1836 ("911 calls commonly trigger police interference with health emergencies."); *see also* Joanna C. Schwartz, *An Even Better Way*, 112 CALIF. L. REV. 1183, 1099-1102 (2024) (describing benefits of disaggregating police functions); Marbre Stahly-Butts & Amna A. Akbar, *Reforms for Radicals? An Abolitionist Framework*, 68 UCLA L. REV. 1544, 1557 (2022) (describing abolitionist efforts "to push the state to shift investments from prisons and police to education, health care, and other forms of what should be a social wage").

[406] *Cf.* Akbar, *supra* note 404, at 1820 (describing how 40% of City of Oakland's budget is devoted to policing).

[407] *See id.* at 1814-15.

[408] *See, e.g.*, Kimberly Kindy, *Some U.S. Police Departments Dump Body-Camera Programs Amid High Costs*, WASH. POST (Jan. 21, 2019), https://www.washingtonpost.com/national/some-us-police-departments-dump-body-camera-programs-amid-high-costs/2019/01/21/991f0e66-03ad-11e9-b6a9-0aa5c2fcc9e4_story.html. However, new technological innovations may ultimately drive these costs down. *See, e.g.*, Tom Simonite, *AI License Plate Readers Are Cheaper—So Drive Carefully*, WIRED (Jan. 27, 2020, 00:00 AM), https://www.wired.com/story/ai-license-plate-readers-cheaper-drive-carefully/.

[409] *See, e.g.*, Jocelyn Simonson, *Copwatching*, 104 CALIF. L. REV. 391, 408-12 (2016); Christina Koningisor, *Public Undersight*, 106 MINN. L. REV. 2221, 2248-66 (2022).

[410] *See, e.g.*, BERKELEY COPWATCH, PEOPLE'S INVESTIGATION: IN-CUSTODY DEATH OF KAYLA MOORE 7 (2013), https://justiceforkaylamoore.files.wordpress.com/2016/07/peoples_investigation_kayla_moore_2013.pdf [https://perma.cc/MQZ7-6NN8] (compiling police statements, reports, and context to describe Kayla Moore's death and recommending policy changes and disciplinary action); IMMIGRANT DEF. PROJECT, ICEWATCH: ICE RAIDS TACTICS MAP 1 (2018), https://www.immigrantdefenseproject.org/wp-content/uploads/ICEwatch-Trends-Report.pdf [https://perma.cc/J3LM-TPAV].

accountable.[411] Such efforts may impose separate privacy costs.[412] Nonetheless, the communities most affected by the harms of policing have the power to determine how best to resolve, weigh, and lessen the impact of such intrusions.[413]

The legislative and judicial branches could also play a more central role in reducing police information-gathering power. State legislatures could ban police use of certain surveillance technologies. Some have already begun to do so—for example, fifteen states have passed restrictions on police use of facial recognition surveillance to identify suspects.[414] Local governments can also play a role. Again, this process is already underway in some places. Seattle, for instance, has introduced mechanisms for ensuring democratic buy-in before police purchase or use of new surveillance technologies.[415]

On the judicial side, judges could take steps to rein in police secrecy, including by scrutinizing law enforcement agencies' claims of potential harm. Such assertions are often accepted at face value, even when speculative or remote.[416] Judges could also abandon the deference doctrines they have adopted in the public records context, easing the judicial barriers that make it more difficult for the public to obtain police records. Consent decrees restricting police surveillance capabilities have also sometimes been effective in the past in constraining police data gathering efforts.[417]

---

[411] *See, e.g.*, ELLEN SACKRISON, WATCH, COURT MONITORING: WATCH'S FIRST LOOK AT RAMSEY COUNTY CRIMINAL COURTS 43-44 (2017), https://www.theadvocatesforhumanrights.org/res/byid/8288 (reporting observations of volunteers sitting in 647 criminal hearings and making recommendations accordingly).

[412] *See, e.g.*, Simonson, *supra* note 409, at 432-33 (describing privacy concerns in context of copwatching efforts, like intrusion of third parties' or arrestees' privacy).

[413] Simonson, *supra* note 373, at 786 (arguing for "new forms of governance arrangements that shift power over policing to those who have historically been the targets of policing").

[414] Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH POL'Y PRESS (Jan. 6, 2025), https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ [https://perma.cc/4RXB-JKFL]; *see also* CAL. PENAL CODE § 832.19 (West 2022). California's biometric surveillance system law expired in 2023, and the state legislature is debating reenacting it. Titus Wu, *California at Crossroads Over Policing and Facial Recognition*, BLOOMBERG L. (Mar. 29, 2023, 5:19 AM), https://news.bloomberglaw.com/privacy-and-data-security/california-at-crossroads-over-policing-and-facial-recognition.

[415] *See, e.g.*, SEATTLE, WASH., MUN. CODE § 14.18.020 (2025) (requiring any government department seeking to obtain surveillance equipment to first obtain permission from City Council).

[416] *See* discussion *supra* notes 243-53 and accompanying text.

[417] *See, e.g.*, Sunita Patel, *Toward Democratic Police Reform: A Vision for "Community Engagement" Provisions in DOJ Consent Decrees*, 51 WAKE FOREST L. REV. 793, 794-95 (2016) (describing effectiveness of consent decrees more broadly).

Better administrative processes might also help.[418] While there has been an administrative turn in policing scholarship in recent years,[419] legal scholars have questioned whether administrative processes can meaningfully constrain police.[420] However, even some skeptics of this broader project have concluded that administrative processes like notice and comment regulation are especially well-suited to the specific task of constraining police surveillance technologies and powers.[421] None of the changes outlined above will be sufficient in isolation.[422] But they could serve as initial steps to help reduce the scope of privacy intrusions imposed by police surveillance and information processing.

Reducing police data collection may involve other tradeoffs. A common claim is that limiting police surveillance powers will increase the risk of crime. This argument is often used to justify enhanced police data collection.[423] It is difficult to address this critique in full. After decades of studying crime, scholars and policymakers still don't know what causes crime rates to rise or fall.[424] They don't even agree on how to define "criminal activity."[425] Further, any single assertion that a reduction in privacy will enhance our security involves a series of counterfactuals that are nearly impossible to prove or disprove.

---

[418] Such reforms should prioritize changes that constrain rather than expand police power. MARIAME KABA, WE DO THIS 'TIL WE FREE US: ABOLITIONIST ORGANIZING AND TRANSFORMING JUSTICE 96 (Tamara K. Nopper ed., 2021) (highlighting "non-reformist reforms," or reforms that "don't make it harder for us to dismantle the systems we are trying to abolish").

[419] *See, e.g.*, Friedman & Ponomarenko, *supra* note 27, at 1833-34 (2015); Barry Friedman, *Secret Policing*, 2016 U. CHI. LEGAL F. 99, 105–09 (arguing law enforcement practices need to be constrained by democratic processes and forces like other government agencies). This new wave of administrative policing scholarship follows an earlier wave from the 1960s and 1970s. For a discussion of this earlier wave, see Ingrid V. Eagly & Joanna C. Schwartz, *Lexipol: The Privatization of Police Policymaking*, 96 TEX. L. REV. 891, 895-96 (2018).

[420] *See, e.g.*, Ponomarenko, *supra* note 389, at 5 ("[T]here are serious reasons to doubt whether rulemaking—either along the lines of the federal model or the proposed alternatives—is in fact a viable strategy for governing the police.").

[421] *See, e.g.*, *id.* at 7 ("[S]ome areas of policing, particularly the use of surveillance technologies, fit comfortably within the rulemaking paradigm . . . .").

[422] *See* Akbar, *supra* note 404, at 1825; *see also* Paul Butler, *The System Is Working the Way It Is Supposed to: The Limits of Criminal Justice Reform*, 104 GEO. L.J. 1419, 1425 (2016) ("[A]ttempts to reform the system might actually hinder the more substantial transformation American criminal justice needs.").

[423] *See* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1609 (2016) (describing safety arguments made to justify new surveillance technology acquisitions).

[424] *See* Matthew Hutson, *The Trouble with Crime Statistics*, NEW YORKER (Jan. 9, 2020), https://www.newyorker.com/culture/annals-of-inquiry/the-trouble-with-crime-statistics (comparing perspectives and findings regarding crime rates and determining data is conflicting and inconclusive).

[425] *Id.*

That said, many of the largest programmatic police surveillance efforts have borne little fruit in terms of increased security. The massive NYPD effort to surveil the Muslim community in the greater New York area after September 11, for example, turned up no meaningful leads after more than six years.[426] The privacy harms imposed by this surveillance are often justified as the price we pay for public safety. But the "public" isn't defined to include everyone. The Muslim community wasn't made safer under the NYPD's surveillance program.[427] Similarly, pervasive police surveillance of Black communities imposes significant safety harms on those same communities.[428] Public safety assessments in the context of pretrial release generally don't account for the interests of the accused or their family.[429] And these harms are exacerbated for Black LGBT people.[430] Even assuming that increased police surveillance results in some measurable increase in public safety—a questionable assumption in and of itself—both the safety benefits and privacy harms are distributed unequally.

B. *Reducing Police Secrecy*

As described above, one way to reduce privacy cooption would be to constrain police data-collection powers. Another would be to minimize police power to keep information secret. But the interplay between these two approaches is important: If we strip police of their power to shield private information from disclosure without reducing their data-collection authority, sensitive information will be at risk. Any reforms to police secrecy powers must be pursued with this concern in mind.

---

[426] Adam Goldman & Matt Apuzzo, *NYPD Muslim Spying Led to No Leads, Terror Cases*, AP (Aug. 21, 2012), https://www.ap.org/ap-in-the-news/2012/nypd-muslim-spying-led-to-no-leads-terror-cases [https://perma.cc/2AJA-J886] ("In more than six years of spying on Muslim neighborhoods, eavesdropping on conversations and cataloguing mosques, the New York Police Department's secret Demographics Unit never generated a lead or triggered a terrorism investigation . . . .").

[427] *See* Saher Khan & Vignesh Ramachandran, *Post-9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear*, PBS NEWS, https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear (last updated Sept. 16, 2021, 5:30 PM) (describing harms imposed on Muslim communities in wake of pervasive police surveillance).

[428] *See* BROWNE, *supra* note 273, at 122 (discussing "racial terror imposed on [B]lack life in America by an overseeing surveillance apparatus" and roots of surveillance).

[429] *See* Okidegbe, *supra* note 360, at 761 ("[E]xclusive reliance on carceral inputs results in these systems obscuring and ignoring the harms associated with a defendant's pretrial detention.").

[430] *See, e.g.*, ARI SHAW, UCLA SCH. OF L. WILLIAMS INST., VIOLENCE AND LAW ENFORCEMENT INTERACTIONS WITH LGBT PEOPLE IN THE U.S. 2 (2020), https://williamsinstitute.law.ucla.edu/wp-content/uploads/LGBT-Violence-Law-Enforce-Mar-2020.pdf [https://perma.cc/F9MU-PHDC] (noting 61% of Black respondents to U.S. Transgender Survey "experienced some form of mistreatment by police").

There are different possibilities for reducing police secrecy power. Legislators could remove decisional control over police records from the police, creating a separate records processing unit insulated from both the decisional and budgetary control of law enforcement actors.[431] An independent processing unit would not have the same incentives to weaponize privacy to advance anti-accountability and other institutional police goals. Breaking out processing responsibilities would place decision-making authority out of the hands of police and divert records processing and administration funds away from police budgets.[432] There is also some precedent for this: some states already place decision-making power in separate institutional bodies when it comes to administrative appeals for records processing decisions, for example.[433]

Legislators could also amend transparency and privacy laws. In the context of police records, such reforms could include revising privacy exemptions to empower victims of police violence and their families with control over records and information relating to the incident, including body camera footage, autopsy records, and photos.[434] Some legislatures have already taken such steps. California, for example, requires police to disclose body camera footage upon request to the subject of the recording, or to their families if the subject is deceased.[435] This strips police of the discretion to invoke a victim's privacy interests against their own wishes or the wishes of their family, at least in the context of certain police records. Whether such material should be made public is a sensitive and difficult question, and victims and the relatives of the deceased should have a formalized role in the decision-making process.

Imposing higher ex ante barriers for police to access private information could help reduce police data collection as well. This could include closing loopholes in federal and state privacy statutes that allow the police exemptions from otherwise applicable privacy rules. The legislative histories of many of these privacy laws reveal that law enforcement agencies routinely testify and comment on draft legislation, while the groups most affected by policing are largely left unrepresented.[436] Bringing these latter voices into the legislative process might help rectify some of these imbalances.

---

[431] *See* Koningisor, *supra* note 19, at 685-87.

[432] *See* Dorothy E. Roberts, *The Supreme Court, 2018 Term—Foreword: Abolition Constitutionalism*, 133 HARV. L. REV. 1, 114 (2019) (arguing in favor of "non-reformist reforms," or efforts to change carceral systems "with the objective of demolishing those systems rather than fixing them").

[433] *See, e.g.*, TEX. GOV'T CODE ANN. § 552.301(a) (West 2023) (requiring agencies to obtain permission from Attorney General's Office before invoking public records exemption).

[434] *Cf.* Okidegbe, *supra* note 360, at 746 (describing how increased transparency without increased decision-making power is insufficient mechanism for change).

[435] CAL. GOV'T CODE § 7923.625(b)(2) (West 2025).

[436] *See* Murphy, *supra* note 12, at 505, 535 ("There is no single NGO or interest group dedicated exclusively to protecting the privacy of the policed poor."); *see also* Wexler, *supra* note 15, at 243-44 ("[O]rganizations that provide indigent criminal defense services and receive federal funding from the Legal Services Corporation are prohibited from lobbying.").

Eliminating overly broad police privacy protections could also rein in privacy cooption at the back end. Police departments have myriad statutory tools available to them to withhold information.[437] Removing expansive and vague privacy carveouts would cut off one source of over-protection. For instance, FOIA and several state public records laws contain separate and stronger privacy protections for police records. Yet these enhanced secrecy powers are not actually required, given the existing privacy carveouts and the panoply of other secrecy tools available to law enforcement agencies.

Broader structural changes to state-level transparency law mechanisms could also help. Strengthening administrative appeals processes would be especially fruitful. Only around half of states have such a mechanism in place; in the other half of states, the only response to police privacy cooption is to sue.[438] Yet doing so is costly and time-consuming, and there are few organizations with the capacity to do so. This is especially true today, when local and regional news outlets are under severe financial pressure.[439] Few are able to sustain such lengthy and expensive public records lawsuits.[440]

Once again, none of these changes will be sufficient in isolation. Reforming the police secrecy regime will require sustained effort and a variety of approaches. Yet such an effort would also yield benefits. Constraining the ability of law enforcement agencies to coopt privacy protections as an anti-accountability tool will reduce the distributive, democratic, and privacy-based harms outlined above.

CONCLUSION

Police are weaponizing privacy protections to shield their own misconduct from public view. This imposes significant costs. It undermines the democratic process, harms oppressed and vulnerable communities, and distorts the public analysis around which privacy harms matter and how best to protect against privacy intrusions. Law enforcement agencies gather vast amounts of information about the public, and the more information they gather, the more persuasive their arguments in favor of police secrecy become. By mapping out the many branches of police privacy powers, this Article helps to illuminate the many costs that privacy cooption imposes.

Further, law enforcement agencies are not the only set of government actors engaged in privacy pretexts. As data privacy protections expand, so do the

---

[437] *See* Koningisor, *supra* note 19, at 637-50 (describing these police secrecy tools).

[438] *See* Koningisor, *supra* note 130, at 1478.

[439] PENELOPE MUSE ABERNATHY & TIM FRANKLIN, NORTHWESTERN MEDILL LOC. NEWS INITIATIVE, THE STATE OF LOCAL NEWS IN 2022, at 5-6 (2022), https://localnews initiative.northwestern.edu/assets/the_state_of_local_news_2022.pdf [https://perma.cc/H72B-W7LG] (documenting challenges local news outlets face and effect this has on communities).

[440] *See* Christina Koningisor & Lyrissa Lidsky, *First Amendment Disequilibrium*, 110 VA. L. REV. 1, 47-48 (2024).

opportunities for government cooption, misuse, and abuse. Additional research into the full scope of public-sector cooption of privacy interests and protections is needed. Such work will bring the problem of privacy cooption by the government into new focus and illuminate paths forward for reform.