ARTICLES

Surveillance and the Tyrant Test

ANDREW GUTHRIE FERGUSON*

How should society respond to police surveillance technologies? This question has been at the center of national debates around facial recognition, predictive policing, and digital tracking technologies. It is a debate that has divided activists, law enforcement officials, and academics and will be a central question for years to come as police surveillance technology grows in scale and scope. Do you trust police to use the technology without regulation? Do you ban surveillance technology as a manifestation of discriminatory carceral power that cannot be reformed? Can you regulate police surveillance with a combination of technocratic rules, policies, audits, and legal reforms? This Article explores the taxonomy of past approaches to policing technologies and—finding them all lacking—offers the "tyrant test" as an alternative.

The tyrant test focuses on power. Because surveillance technology offers government a new power to monitor and control citizens, the response must check that power. The question is how, and the answer is to assume the worst. Power will be abused, and constraints must work backwards from that cynical starting point. The tyrant test requires institutional checks that decenter government power into overlapping community institutions with real authority and enforceable individual rights.

The tyrant test borrows its structure from an existing legal framework also designed to address the rise of a potentially tyrannical power—the U.S. Constitution and, more specifically, the Fourth Amendment. Fearful of a centralized federal government with privacy invading intentions, the Fourth Amendment—as metaphor and methodology—offers a guide to approaching surveillance; it allows some technologies but only within a self-reinforcing system of structural checks and balances with power centered in opposition to government. The fear of tyrannical power motivated the original Fourth Amendment and still offers lessons for how society should address the growth of powerful, new surveillance technologies.

* Professor of Law, American University Washington College of Law. Thank you to the commentators at the 2021 Privacy Law Scholars Conference and to my co-panelists at the Association of American Law Schools Conference panel on Deep Surveillance. Thank you to commentators at the inaugural meeting of the Columbia University Sociology of Algorithms Workshop.

TABLE OF CONTENTS

INTRODUCTION

Surveillance is being mainstreamed into everyday life.[1] Consumer surveillance sounds with every swipe of a smartphone.[2] Social media surveillance links us by every share, like, and click.[3] Public safety surveillance is changing how governments monitor protests and disorder.[4] The digital clues of life are being mined, monetized, and monitored in unprecedented ways.[5]

Law enforcement has embraced this development, capturing these digital trails and capitalizing on the insights available.[6] Data-driven policing has moved from theory into practice with rapid speed.[7] Predictive policing technologies target high-risk neighborhoods and people.[8] Video analytics, police body cameras, and automated license plate readers record movement and travel.[9] Mass aerial surveillance

1. *See, e.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 3 (2014) ("We are living in a Dragnet Nation—a world of indiscriminate tracking where institutions are stockpiling data about individuals at an unprecedented pace.").

2. *See* Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

3. *See* Rachel Levinson-Waldman, *Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media*, 71 OKLA. L. REV. 997, 998 (2019) ("[P]olice are using social media not only to send information out to the public but also to keep track of what people are doing both online and off.").

4. *See, e.g.*, Matthew Guariglia, *How to Identify Visible (and Invisible) Surveillance at Protests*, ELEC. FRONTIER FOUND. (Nov. 5, 2020), https://www.eff.org/deeplinks/2020/06/how-identify-visible-and-invisible-surveillance-protests [https://perma.cc/3ANB-AF7C]; Caroline Haskins, *Almost 17,000 Protesters Had No Idea a Tech Company Was Tracing Their Location*, BUZZFEED (June 25, 2020, 2:40 PM), https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying [https://perma.cc/X4LQ-DPRS].

5. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019).

6. *See generally* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) (describing how new technology is changing how police do their jobs); DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017) (recognizing that new surveillance technologies allow law enforcement officers to track citizens, and revealing how the Fourth Amendment can provide security in an age of increasing government surveillance).

7. Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 113 (2017) (describing the rise of data-driven policing technologies).

8. *See, e.g.*, Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1143–44 (2017).

9. *See* JAY STANLEY, ACLU, THE DAWN OF ROBOT SURVEILLANCE: AI, VIDEO ANALYTICS, AND PRIVACY 17–19 (2019), https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf [https://perma.cc/6E9Q-YBXF] (discussing video analytics); Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 U.C. DAVIS L. REV. 897, 908 (2017) (discussing police body cameras); Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 285–87 (discussing automatic license plate recognition surveillance).

and localized drones monitor criminal incidents.[10] Location-tracking devices, the "Internet of Things,"[11] smart cars, and a host of digital devices provide fresh clues for law enforcement officers investigating crimes.[12] And, all of this information is being gathered in growing, aggregated databases to be mined, manipulated, and studied by powerful computer analytics to identify evidence useful in criminal prosecutions.[13]

Each of these policing technologies has fueled a fight between privacy advocates and law enforcement professionals, with an almost predictable pattern of suspicion, scandals, and setbacks following each new innovation. The debate swirls without finding shared first principles[14] from which to chart a way forward. Privacy and racial-justice advocates see little reason to concede anything to "surveillance creep" at this early stage of the rhetorical battle over use of surveillance technology. Similarly, police—convinced of the value of powerful monitoring capabilities—have shown little interest in filling the legal void with voluntary regulations. Finally, moderate voices seeking to regulate, reform, and curtail the growth of surveillance find themselves criticized from all sides for being too accommodating to police (and thus fueling oppression) or too bureaucratic in practice (and thus stifling innovation).

Facial recognition technology offers a recent example of this tension. Among many era-defining mass surveillance technologies, facial recognition has arisen as a flash point for a heated national debate.[15] Police have embraced the

10. *See* Chris Francescani & Aaron Katersky, *The NYPD, the Nation's Largest Police Department, Puts Its Eyes in the Skies with New Drone Program*, ABC NEWS (Dec. 4, 2018, 4:00 PM), https://abcnews.go.com/Technology/nypd-nations-largest-police-department-puts-eyes-skies/story?id=59599207 [https://perma.cc/9EX5-JBCC]; Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/; Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST (Feb. 5, 2014), https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.

11. Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986; *see also* Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1599 (2014) ("The 'Internet of Things' is . . . a term used to describe the array of internet-enabled devices (like cars and traffic lights but also coffee pots and clothes) that are entering our everyday lives. These devices not only collect increasingly specific personal information; but they also can share that data with other people and other devices." (footnote omitted)).

12. *See, e.g.*, Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 819–20 (2016) (cataloging the rise of digital tracking sensor devices).

13. *See* Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score,'* WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html; Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. L. & SOC. SCI. 293, 294 (2018).

14. I use the term *first principles* to explain a worldview or attitude toward policing technologies.

15. Facial recognition threatens to become a constant, privacy-eviscerating technology that captures images without notice, identifies people in public, and chills protected First Amendment protest activities. As such, it has captured national attention and concern when used by police. *See* CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, GEORGETOWN L. CTR. ON PRIV. & TECH., THE

technology to identify criminal suspects mostly without legal limits.[16] In response, facial recognition abolitionists have sought a complete ban on the technology (or, at a minimum, a moratorium on its use).[17] These advocates believe that regulation concedes too much—that a regulated police "superpower" is never going to actually be limited in practice.[18] Such positioning stakes out first principles around the inability to regulate police power and thus the need for a complete ban. After all, a dystopia with thoughtful regulation is still a dystopia.

This divide on first principles has been the unspoken battle around all new policing technologies. Without a shared stance on how to approach the promise and the threat of new surveillance technology, we lack a constructive starting point from which to move forward. The question of "where we go next with policing" keeps getting thwarted by where we start.

This Article seeks to reset the starting point for the debate on policing technologies. Specifically, this Article reexamines the question of first principles, offering four framing lenses to examine the different ways society has approached new policing powers.[19] These lenses are: (1) the trust lens, (2) the trap lens, (3) the technocratic lens, and (4) the tyrant lens; together they offer a rough taxonomy to analyze all future police surveillance technologies. The hope is to provide a descriptive and theoretical framework to evaluate the best approach to new surveillance technologies used by the police.

The trust lens has been our default model to regulate policing technology for much of the century. With some exception, most policing technologies remain unregulated on a federal, state, or local level, allowing police to develop best practices on a theory that expertise is a reason to trust police.[20] Companies invent a new surveillance technology, sell the technology to police, and then police operate it without significant formal accountability, oversight, or transparency

---

PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (2016); *see also* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1167–91 (2021) (discussing the legal and ethical debate over facial recognition).

16. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 4:19 AM), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/HMV7-HYMU].

17. *See* Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771; Tawana Petty, *Defending Black Lives Means Banning Facial Recognition*, WIRED (July 10, 2020, 8:00 AM), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition.

18. *See* Hamid Khan & Peter White, *Police Surveillance Can't Be Reformed. It Must Be Abolished*, VICE (Mar. 10, 2021, 10:36 AM), https://www.vice.com/en/article/xgzj7n/police-surveillance-cant-be-reformed-it-must-be-abolished [https://perma.cc/WKS6-D6HL].

19. The different lenses discussed are not mutually exclusive and include some overlap, but they offer framing mechanisms to see the underlying philosophy of how some groups have approached the problem of new surveillance technologies.

20. *See* Barry Friedman & Elizabeth G. Jánszky, *Policing's Information Problem*, 99 TEX. L. REV. 1, 30 (2020) ("In most states, invasive technologies like drones, license plate readers, and predictive policing algorithms remain unregulated altogether. Any sort of legislative regulation of policing is patchwork and episodic at best." (footnote omitted)).

mechanisms.[21] Predictive policing algorithms, automated license plate readers, video analytics, gunshot sensors, stingray devices, drones, robots, and other innovations have grown from an interesting idea to government adoption without significant regulation or public oversight.[22] The default position of those who adopt the trust lens has been to maintain a healthy, hands-off approach to regulation. Trust is placed in the underlying incentives of public safety priorities.[23] Most policing technologies easily pass the trust test, if you start with faith in law enforcement.

In contrast to the trust lens, the trap lens involves the fear that giving police any new surveillance power is a trap that will essentially create new social control methods to be used against the less powerful. The trap is set by providing seemingly new innovations under the guise of progress or objectivity. The trap springs when those technologies reify existing social hierarchies, structural power dynamics, and racial bias. The trap lens looks over the long history of policing in America and says there are no good counterexamples when police power was not used against racial minorities and the poor.[24] Policing is the problem, and high-tech policing will not solve the underlying power dynamics.[25] The movement to "abolish the police" is in large measure a response to this distrust.[26] The argument

21. *See generally* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1595 (2016) (using case studies from Seattle, Oakland, and San Diego to "comprehensively consider the intersection of procurement and local surveillance policy making"); Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 20 (2017) ("Private surveillance technology companies wield an undue influence over public police today in ways that aren't widely acknowledged, but have enormous consequences for civil liberties and police oversight.").

22. For more on the impact of big data policing technologies, see generally FERGUSON, *supra* note 6.

23. *See* Robin K. Magee, *The Myth of the Good Cop and the Inadequacy of Fourth Amendment Remedies for Black Men: Contrasting Presumptions of Innocence and Guilt*, 23 CAP. U. L. REV. 151, 157, 160–61 (1994) (describing the "good cop paradigm" and the "false myth of the police officer as a law-abiding citizen who is chiefly, if not totally, motivated by law enforcement interests when appropriate and who can be trusted to behave within constitutional parameters" (footnote omitted)).

24. As will be discussed in Part II, throughout history, American policing protected capital, white property, and cultural norms that constrained Black economic or social power. *See generally* PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN 59–61 (2017); ALEX S. VITALE, THE END OF POLICING (2018).

25. *See* 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 [https://perma.cc/5BMF-C9DD]; Dorothy Roberts & Jeffrey Vagle, Opinion, *Racial Surveillance Has a Long History*, HILL (Jan. 4, 2016, 5:11 PM), http://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history [https://perma.cc/R5WL-DQHG].

26. The abolitionist movement and those who advocate to abolish policing, police surveillance, and other forms of carceral restraint have created a rich literature of theory and practical advice. *See, e.g.*, MARIAME KABA, WE DO THIS 'TIL WE FREE US: ABOLITIONIST ORGANIZING AND TRANSFORMING JUSTICE 4–5 (Tamara K. Nopper ed., 2021); Mariame Kaba, Opinion, *Yes, We Mean Literally Abolish the Police*, N.Y. TIMES (June 12, 2020), https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html. The trap lens framework does not seek to incorporate or be incorporated into this existing literature. Instead, the trap lens offers a generic term to address some of the same concerns arising from this movement.

is to keep surveillance powers completely out of the hands of police because police cannot abuse technology that they do not have (or that does not exist).[27]

The technocratic lens evolved as a counterweight to the trust and trap paradigms. Led by civil society groups and academics, the idea that rules; structures; and sustained, front-end accountability must go into the adoption of new technology is growing.[28] Toolkits, policies, and local legislative accountability laws have been adopted.[29] The technocratic lens emphasizes ex ante rules, transparent policies, and audits as external accountability mechanisms to address potential misuse. In addition, this approach embraces existing law and remains conscious of the legal, social-economic, and racial realities when technology interacts with an unequal society. If the trust lens defaults to a defense that "technology is a tool to be used for good," the technocratic lens defaults to a defense that "an unregulated tool is a dangerous tool." The technocrat's solution involves detailed use policies, audits, legal remedies, and a level of expert oversight and engagement to address concerns about accountability, transparency, bias, and misuse. A policing technology only passes the technocratic test if a system of accountability, transparency, and rulemaking has been designed to regulate it with appropriate democratic authorization.

Trust, trap, and technocratic perspectives offer three approaches to surveillance technology. But, as will be discussed, they are all inadequate to the task. This Article offers a fourth alternative—the tyrant lens. The tyrant lens assumes that the technology will be misused by a metaphorical tyrant and focuses on centering power away from the government and into the hands of the people. The tyrant lens is not framed as an absolute ban on technologies (like the trap lens) nor a mere reform (like the technocratic lens), but it fits somewhere in between. The tyrant lens starts with a structural suspicion of government power and works

27. *Cf.* RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 184 (2019) (noting that "computer programmers and others in the tech industry are beginning to recognize their complicity in making the New Jim Code possible").

28. This technocratic lens is an inexact category for scholars who have approached the problem of policing from various democratic or administrative approaches. This category might include what Professor Andrew Crespo and Professor Wayne Logan have called the "New Administrativists." *See* Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049, 2057–59 (2016); Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L.J. 369, 386 (2018) ("[S]everal scholars have urged that courts defer to rules regulating police when the rules result from local executive and quasi-executive entities."); *see also* Mailyn Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 SANTA CLARA HIGH TECH. L.J. 481, 555 (2020); Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1874–75 (2015); Maria Ponomarenko, *Rethinking Police Rulemaking*, 114 NW. U. L. REV. 1, 51–56 (2019); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1043 (2016); Selbst, *supra* note 7, at 117; Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 120–21 (2016). These scholars are not necessarily focused on police technologies (although some are) but instead on the power to regulate policing via administrative and technocratic means.

29. As will be discussed in Part III, academics and civil rights groups have developed a handful of white papers and toolkits to assist police departments and city governments about how to address the threats of new surveillance technologies. *See infra* Section III.B.4.

backwards from that distrust with overlapping checks and balances, and rights and remedies built within the authorizing legislation.

The tyrant lens (or what I will call the tyrant test) borrows its structure from an existing legal framework also created to address the rise of tyrannical power—the U.S. Constitution and, more specifically, the Fourth Amendment.[30] Fearful of a centralized government with privacy-invading powers, the Fourth Amendment —as metaphor and methodology—offers a helpful guide to allow some policing technologies but only within a self-reinforcing system of structural limitations with power centered in opposition to government.[31] As a first principle, the tyrant test needs a structural approach, distrusting malleable, executive branch policies and requiring an entire system of interlocking power centers, checks and balances, community institutions, and rights-based remedies. This was the initial hope of the Fourth Amendment's drafters who faced a history of real tyranny and had a goal to situate power in the hands of citizens.[32] While the Fourth Amendment in modern practice has failed to restrain government power, as metaphor, the tyrant test crystalizes the goal of designing a systemic and citizen-based response to government surveillance. As practical methodology, it frames technocratic solutions and trap concerns into an enforceable legal framework with powers outside of the executive branch.

A form of tyranny also motivated the ratification of the Fourteenth Amendment.[33] The arbitrary and oppressive police powers of slave catchers and the first Southern police forces directly influenced those who ratified the Reconstruction Amendments.[34] A modern understanding of the Fourth Amendment must incorporate this fear of racial tyranny by lawful police authority, a fear shared by modern police abolitionists and the original antislavery abolitionists.

This Article explores these four first-principle lenses. Part I begins with an analysis of the trust lens, examining how the default position of trusting the police evolved as the dominant position around new police surveillance tech. This Part also examines why this trust has been misplaced and looks at two specific examples of big data policing in Los Angeles and Chicago. Part II examines the trap lens and how surveillance has been misused against those with less social, economic, and cultural power. The analysis foregrounds current debates about abolishing police surveillance technology against an examination of America's long history of racially biased police surveillance. Part III examines the rise of a technocratic response to surveillance reform. The technocratic lens blends democratic

30. U.S. CONST. amend. IV.

31. Part IV details the justification for basing the tyrant test on a Fourth Amendment framework.

32. *See* Magee, *supra* note 23, at 190 ("The limitation on government expressed in the Fourth Amendment was a rational response informed by the intense history of political oppression and tyranny by the British Crown over the colonists and outspoken subjects of Britain proper.").

33. U.S. CONST. amend. XIV.

34. *See* ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE, 1789–1868, at 256 (2006); Andrew E. Taslitz, *Slaves No More!: The Implications of the Informed Citizen Ideal for Discovery Before Fourth Amendment Suppression Hearings*, 15 GA. ST. U. L. REV. 709, 748 (1999) (discussing the link between policing slavery and Fourth Amendment principles).

accountability principles with policy proscriptions to rebalance the excesses and errors of unregulated technology, but, as will be discussed, it ultimately fails to offer a sufficient check on police power. Finally, Part IV details the tyrant test as a new response to growing police surveillance. By presuming the technology will be abused by a metaphorical tyrant, legal and institutional power structures can be developed to limit the potential harms before use.

Each Part addresses the justification, results, limitations, and promise of these different first principle approaches. Each also evaluates whether any of the tests are sufficient to answer the fundamental question of whether it is possible to regulate new, liberty-eroding police surveillance technologies. This Article argues that, although likely unsatisfying to trust, trap, and technocratic adherents, the tyrant test offers the best way forward to allow some policing technologies within limits.

I. THE TRUST LENS

Policing technology operates on a trust basis.[35] Despite ample examples of police misconduct[36] and abuse,[37] most police departments operate without significant oversight and with the benefit of trust. Even police departments operating under federal consent decrees[38] or cities that have faced protests to defund the police[39] still allow surveillance technologies to exist mostly unregulated, unexamined, and unfettered. Trust is the default for policing, and this is especially true when it comes to new surveillance technologies.

A. WHY DEFAULT TO TRUST?

Unpacking why police have been trusted to use surveillance technologies without substantial oversight is complicated by the fragmented nature of policing.[40]

---

35. *See* Rachel Moran, *In Police We Trust*, 62 VILL. L. REV. 953, 966–68, 993 (2017) (detailing the history of Supreme Court deference to police power in the later part of the twentieth century).

36. *See, e.g.*, Rachel A. Harmon, *Promoting Civil Rights Through Proactive Policing Reform*, 62 STAN. L. REV. 1, 2 (2009) ("Much police misconduct is not accidental, incidental, or inevitable. Instead, it is systemic, arising out of departmental deficiencies that undermine officer adherence to legal rules."); Laurie L. Levenson, *Police Corruption and New Models for Reform*, 35 SUFFOLK U. L. REV. 1, 4–10 (2001) (detailing a long history of police corruption).

37. *See, e.g.*, Hallie Ryan & Jon Greenbaum, *Though the Technology Is New, Police Abuse Is Not*, 42 HUM. RTS. no. 1, 2016, at 1, 22 (2016); David Rudovsky, *Police Abuse: Can the Violence Be Contained?*, 27 HARV. C.R.-C.L. L. REV. 465, 466 (1992).

38. For example, Baltimore, Maryland, was under a federal consent decree when it adopted a pilot program of Pervasive Surveillance System planes. *See* CIV. RTS. DIV., DOJ, INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 11 (2016); *see also* Kevin Rector, *Baltimore Surveillance Flight Data Suggest Homicides, Shootings Were Captured*, BALT. SUN (Oct. 7, 2016, 4:30 PM), http://www.baltimoresun.com/news/maryland/investigations/bs-md-sun-investigates-surveillance-dates-20161007-story.html [https://perma.cc/N6SK-NCAC] (reporting that the Baltimore police's "aerial surveillance plane" flew above the city during "at least nine homicides and 21 shootings").

39. New York City, Los Angeles, Baltimore, and Chicago have all seen defund the police protests and yet all have significantly invested in big data policing systems. *See infra* notes 61, 174.

40. *See* Mark Berman, *Most Police Departments in America Are Small. That's Partly Why Changing Policing Is Difficult, Experts Say.*, WASH. POST (May 8, 2021, 4:59 PM), https://www.washingtonpost.com/nation/2021/05/08/most-police-departments-america-are-small-thats-partly-why-changing-policing-is-difficult-experts-say/.

With almost 18,000 different law enforcement entities in the United States, it is difficult to make generalizations.[41] But the tiny number of localities that require any independent oversight of police surveillance proves the point that most cities do little but hope that the police use the technologies appropriately.[42] Seattle, Oakland, San Francisco, Santa Cruz, New York, and a few smaller cities have (after years of advocacy) adopted local surveillance oversight ordinances.[43] Most others have no regulation.

This Section breaks down the trust lens, examining why many jurisdictions have defaulted to a trust lens for viewing policing technologies. While not an exclusive list, reasons of tradition, professionalism, tactical secrecy, capacity, political power, and procurement policies all act to insulate police technology from significant oversight.

1. Tradition

Traditionally, police have been allowed to innovate without much public accountability. New weapons,[44] new communication systems,[45] and new policing tactics[46] have all been adopted without significant public input. While scholars can debate whether police—as an institution—are overregulated or underregulated,[47] there is little question that new technologies over the past decades have

41. *See* Alan Z. Rozenshtein, *Wicked Crypto*, 9 U.C. IRVINE L. REV. 1181, 1208 (2019) ("[T]he vast majority of crime, and the vast majority of law enforcement investigations, occur within the jurisdiction of the nearly 18,000 state, county, and local police departments and law-enforcement agencies across the country.").

42. The Samuelson Law, Technology, & Public Policy Clinic at University of California, Berkeley Law School recently published an excellent white paper analyzing sixteen localities that have attempted formal oversight mechanisms. ARI CHIVUKULA & TYLER TAKEMOTO, SAMUELSON L., TECH. & PUB. POL'Y CLINIC, LOCAL SURVEILLANCE OVERSIGHT ORDINANCES (2021), https://www.law.berkeley.edu/wp-content/uploads/2021/02/Local-Surveillance-Ordinances-White-Paper.pdf [https://perma.cc/NH6K-JHW5].

43. *See* Fidler, *supra* note 28, at 545 & n.274 (noting that "[a]s of August 2020, fourteen local government entities—thirteen cities and one county—have passed laws formalizing administrative control over police use of sophisticated investigative technologies," and providing citations to local ordinances); *see also* Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 1982–2020 (2018) (providing a detailed example of the role of privacy ordinances in Seattle and New York City).

44. For a fascinating look at how police adopt new police surveillance technologies, see MATT STROUD, THIN BLUE LIE: THE FAILURE OF HIGH-TECH POLICING 91–128 (2019) (describing how tasers were adopted across America).

45. *See, e.g.*, Phil Goldstein, *NG911 Technology: What State and Local Communities Need to Know*, STATETECH (Sept. 13, 2019), https://statetechmagazine.com/article/2019/09/ng911-technology-what-state-and-local-communities-need-know-perfcon [https://perma.cc/4H9M-MBXV].

46. *See, e.g.*, Brandon Garrett & Seth Stoughton, *A Tactical Fourth Amendment*, 103 VA. L. REV. 211, 246–52 (2017) (detailing the changes of police use of force over time); Seth W. Stoughton, *Principled Policing: Warrior Cops and Guardian Officers*, 51 WAKE FOREST L. REV. 611, 666–67 (2016) (discussing the evolution of a "[g]uardian" approach to policing as opposed to a "[w]arrior" approach).

47. There is a wealth of scholarship discussing the ways police are regulated. *See, e.g.*, Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 764 (2012); Lawrence Rosenthal, *Good and Bad Ways to Address Police Violence*, 48 URB. LAW. 675, 678 (2016); Frank Rudy Cooper, *A Genealogy of Programmatic Stop and Frisk: The Discourse-to-Practice-Circuit*, 73 U. MIA. L. REV. 1,

been adopted without significant regulatory limits.[48] Data-driven innovations such as CompStat in New York[49] and predictive policing in Los Angeles[50] were adopted because a nationally known police leader, William Bratton, promoted the idea.[51] Video surveillance systems,[52] drones,[53] audio sensors,[54] and automated license plate readers[55] have encircled major cities such as Chicago, Detroit, and New York with little public notice.[56] Data-driven platforms control operation centers and shape investigations with few external oversight mechanisms.[57] The default has been to allow police to make decisions they thought were best for their institutions, personnel, and communities.

2. Professionalism

This traditional deference rests in part on the perceived professionalism of police.[58] As a general matter, police departments in America are insular

31–32 (2018); Stephen Rushin & Griffin Edwards, *De-Policing*, 102 CORNELL L. REV. 721, 736–38 (2017); Seth W. Stoughton, *The Incidental Regulation of Policing*, 98 MINN. L. REV. 2179, 2182 (2014).

48. *See supra* notes 42–43 and accompanying text.

49. James J. Willis, Stephen D. Mastrofski & David Weisburd, *Making Sense of COMPSTAT: A Theory-Based Analysis of Organizational Change in Three Police Departments*, 41 LAW & SOC'Y REV. 147, 148 (2007).

50. Caroline Haskins, *Dozens of Cities Have Secretly Experimented with Predictive Policing Software*, VICE (Feb. 6, 2019, 10:00 AM), https://www.vice.com/en_us/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software [https://perma.cc/99TH-QV6J].

51. *See* Ferguson, *supra* note 8, at 1126.

52. *See, e.g.*, Eoin Higgins, *Pre-Crime Policing Is Closer than You Think, and It's Freaking People Out*, VICE (June 12, 2018, 3:47 PM), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-many-cameras-precrime [https://perma.cc/3N7G-HTSW].

53. *See How Law Enforcement Can Harness the Benefits of an Unmanned Aircraft Systems (UAS) Program*, NAT'L INST. JUST. (Dec. 15, 2016), https://www.nij.gov/topics/law-enforcement/operations/aviation/Pages/harnass-benefits-of-unmanned-aircraft-systems.aspx [https://perma.cc/3UFU-GCE8] ("According to the Bureau of Justice Statistics, only about 350 law enforcement agencies in the U.S. had aviation programs in active use.").

54. *See, e.g.*, Cale Guthrie Weissman, *The NYPD's Newest Technology May Be Recording Conversations*, INSIDER (Mar. 26, 2015, 1:05 PM), http://www.businessinsider.com/the-nypds-newest-technology-may-be-recording-conversations-2015-3 [https://perma.cc/8V78-3EQY].

55. *See* Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/.

56. *See* JOHN S. HOLLYWOOD, KENNETH N. MCKAY, DULANI WOODS & DENIS AGNIEL, RAND CORP., REAL-TIME CRIME CENTERS IN CHICAGO: EVALUATION OF THE CHICAGO POLICE DEPARTMENT'S STRATEGIC DECISION SUPPORT CENTERS 36, 38 (2019) (Chicago); *Project Green Light Detroit*, CITY OF DETROIT, https://detroitmi.gov/departments/police-department/project-green-light-detroit [https://perma.cc/ZX77-UHH9] (last visited Sept. 11, 2021) (Detroit); Colleen Long, *NYPD, Microsoft Create Crime-Fighting Technology; City Could Make Millions in Business Deal*, YAHOO! NEWS (Feb. 20, 2013), https://news.yahoo.com/nypd-microsoft-create-crime-fighting-technology-city-could-033128315.html [https://perma.cc/V3KN-P8RK] (New York City).

57. *See* Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOCIO. REV. 977, 987 (2017); Matt McFarland, *A Rare Look Inside LAPD's Use of Data*, CNN (Sept. 11, 2017, 11:42 AM), https://money.cnn.com/2017/09/11/technology/future/lapd-big-data-palantir/index.html [https://perma.cc/F97A-JX3W].

58. *See* CHRISTOPHER STONE & JEREMY TRAVIS, HARV. KENNEDY SCH. & NAT'L INST. OF JUST., TOWARD A NEW PROFESSIONALISM IN POLICING 11–12, 14–15 (2011) (describing a push for a "[n]ew [p]rofessionalism" in policing).

institutions with specialized training academies,[59] hierarchical command structures,[60] and broad authority to reduce crime rates.[61] Police officers operate with a significant level of autonomy due to their perceived training and experience.[62] Although accountable to a politically appointed or elected chief of police,[63] the complexity of managing a large institution tasked with a wide-ranging set of responsibilities has led to significant deference to professional judgments.[64] The thinking is that police know "police stuff," and this deference to expertise carries over to technology. After all, if we trust police to enforce the law, why would we not also trust them with the technology to support those law enforcement policy goals? While unthinking deference has been eroded in recent years with protests over police misconduct and video evidence of brutality,[65] police have managed their operations with a high level of independence for decades.[66]

---

59. *See* Garrett & Stoughton, *supra* note 46, at 250 (describing use of force training, and noting that "[a]s of 2013, the most recent year for which data are available, about 45,000 police recruits enrolled in, and about 38,600 graduated from, one of the more than 650 police academies scattered across the country, where they received an average of 840 hours of training"); *see also* Yuri R. Linetsky, *What the Police Don't Know May Hurt Us: An Argument for Enhanced Legal Training of Police Officers*, 48 N.M. L. REV. 1, 14–19 (2018) (providing a brief history about police training).

60. *See* Catherine L. Fisk & L. Song Richardson, *Police Unions*, 85 GEO. WASH. L. REV. 712, 722 (2017) ("Police departments are hierarchical, with a chain of command as in the military and a sharp division between the leadership and the rank-and-file." (footnote omitted)).

61. *See* Barry Friedman, *Disaggregating the Policing Function*, 169 U. PA. L. REV. 925, 949–54 (2021) [hereinafter Friedman, *Disaggregating*] (describing research into actual police responses to criminal activity); Barry Friedman, *Secret Policing*, 2016 U. CHI. LEGAL F. 99, 106–07 [hereinafter Friedman, *Secret Policing*] ("Most policing agencies operate under extraordinarily broad delegations of authority that instruct them only to enforce the substantive laws.").

62. *See* Anna Lvovsky, *The Judicial Presumption of Police Expertise*, 130 HARV. L. REV. 1995, 2006 (2017) ("Where did police officers derive their expert insights? One source was basic experience: the instinctive wisdom about criminal activity gathered through an officer's exposure to the streets.").

63. *See* Friedman & Ponomarenko, *supra* note 28, at 1831 (describing how "police chiefs typically serve at the pleasure of the mayor, police commission, or city council, and sheriffs are directly elected by the people").

64. Elizabeth E. Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CALIF. L. REV. 199, 206 (2007) ("The exercise of discretion results from influences on the police both at the organizational and individual level. At the organizational level, local police department [sic] must choose some 'priorities of enforcement' over others. These choices reflect social and political choices that prevent a police organization from 'full enforcement:' enforcing the law every time a violation is observed." (footnotes omitted) (quoting Joseph Goldstein, *Police Discretion Not to Invoke the Criminal Process: Low-Visibility Decisions in the Administration of Justice*, 69 YALE L.J. 543, 559–61 (1960))).

65. *See, e.g.*, Nick Statt, Nicole Wetsman, Sarah Jeong, James Vincent, Cameron Faulkner, Ashley Carman, Monica Chin, Justine Calma, Loren Grush, Megan Farokhmanesh & Russell Brandom, *The Peace Reporters: The Police Dressed for War. The People Showed Up with Cameras.*, VERGE, https://www.theverge.com/21355122/police-brutality-violence-video-effects-trauma-civil-rights-black-lives-matter [https://perma.cc/37PC-REVL] (last visited Oct. 13, 2021).

66. *See generally* Lvovsky, *supra* note 62, at 2066 (critiquing the rise of a presumption of police expertise); Samuel Walker, *Governing the American Police: Wrestling with the Problems of Democracy*, 2016 U. CHI. LEGAL F. 615, 629 (critiquing the rise of professionalism in the context of studying the history of policing in America).

3. Tactical Secrecy

Such deference is especially true when the technology is used as part of tactical operations that rely on secretive surveillance. Monitoring technology is arguably less effective when the surveilled subject is aware of the monitoring.[67] While some forms of surveillance technology are meant to deter crime, police usually seek to keep the tactical surveillance systems secret.[68] Further, the proprietary nature of the technology adds pressure to keep many types of police surveillance opaque.[69] In some extreme cases, police have signed nondisclosure agreements with the private companies forbidding the government from revealing the existence of the technology, even to judicial authorities.[70] The alignment of tactical secrecy and corporate secrecy has been a powerful force against transparency and accountability in the criminal justice system.[71]

4. Capacity

Trust is not just a reflection of expertise but also a reflection of oversight capacity. Few institutions or people have the capacity to conduct oversight over the police and fewer still can analyze police surveillance technologies. In many cities, the issue is not just that police do not want oversight but that no entity has the resources and capacity to conduct the type of oversight necessary.[72] When sophisticated and proprietary technology is involved, this oversight role is even more difficult because the underlying information is complex and hard to obtain. The entities that have the capacity to audit data-driven systems or examine the legal risks of surveillance are few in number.[73] The result is that without forcing

67. *See* Friedman, *Secret Policing*, *supra* note 61, at 120–21 ("Policing . . . is like a game of cat and mouse—as the cats get smarter, the mice adapt. The longer police are able to keep their investigative strategies secret, the longer they can maintain the upper hand.").

68. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 34 (2004) ("[L]aw enforcement benefits in several ways from the secrecy of its surveillance. The less people know about surveillance, the more information surveillance reveals and the less law enforcement needs to spend on counter-surveillance efforts.").

69. *See generally* Crump, *supra* note 21 (discussing secret acquisition of surveillance equipment by police); Joh, *supra* note 21 (discussing the erosion of transparency caused by private surveillance company influence on policing).

70. *See* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 39 (2016) ("Nondisclosure agreements bar police departments adopting the technology from disclosing 'any information' relating to the surveillance equipment to any third parties, private and public." (footnote omitted)); Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 515 (2019) (discussing nondisclosure agreements).

71. *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2028 (2017); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1395 (2018).

72. *See, e.g.*, Rubinstein, *supra* note 43, at 1987–91 (detailing the complexity and difficulty of local surveillance oversight in Seattle).

73. Academic institutions and civil liberties groups have interest, expertise, and capabilities, but only a handful of groups can do it at the scale needed. *See, e.g.*, *About EFF*, ELEC. FRONTIER FOUND., https://www.eff.org/about [https://perma.cc/LL74-8CC2] (last visited Oct. 13, 2021) ("EFF advises policymakers and educates the press and the public through comprehensive analysis, educational guides, activist workshops, and more."); *Our Mission*, POLICING PROJECT, https://www.policingproject.org/our-

mechanisms to make those audits occur (and to pay for them), the accountability processes simply do not happen. In many ways, trusting the police becomes the default when there is no other alternative.

5. Political Power

A lack of capacity to conduct oversight is not accidental. Police have long used political means to fight accountability measures.[74] While surveillance technology is relatively new, the consolidation of police power and the resultant avoidance of accountability is not. For decades, in local elections, it was imperative for local politicians to have the backing of the police.[75] This proximity to power discouraged robust oversight over policing and led to a culture of unaccountability in some police departments. Police unions furthered this hands-off approach to oversight.[76] Further, politicians and police were mostly aligned in wanting more surveillance as an effort to sell a vision of crime reduction and even shape how "crime" is defined.[77] In many instances, city officials could see trusting police as helpful to their political self-interest.[78]

6. Procurement

Finally, the rules governing police procurement (including buying new technologies) encouraged opaqueness around surveillance. In some cases, the local

mission [https://perma.cc/C9CW-N94F] (last visited Oct. 13, 2021) ("We Partner With Communities And Police To Promote Public Safety Through Transparency, Equity, and Democratic Engagement."); *Privacy and Surveillance*, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance [https://perma.cc/CGW9-JJ6Z] (last visited Oct. 13, 2021) ("The ACLU has been at the forefront of the struggle to prevent the entrenchment of a surveillance state . . . .").

74. *See* Samuel Walker, *The New Paradigm of Police Accountability: The U.S. Justice Department "Pattern or Practice" Suits in Context*, 22 ST. LOUIS U. PUB. L. REV. 3, 11–12 (2003) ("[G]enerations of police managers have strenuously fought the actual or threatened intrusions into their managerial prerogatives, whether by the U.S. Supreme Court, citizen oversight agencies, or police unions."); *see also* Benjamin Levin, *What's Wrong with Police Unions?*, 120 COLUM. L. REV. 1333, 1400 (2020) ("Police unions have fought to shield their members from public scrutiny and legal accountability.").

75. *See, e.g.*, Lonnie T. Brown, Jr., *Different Lyrics, Same Song: Watts, Ferguson, and the Stagnating Effect of the Politics of Law and Order*, 52 HARV. C.R.-C.L. L. REV. 305, 320, 338 (2017).

76. *See generally* Fisk & Richardson, *supra* note 60, at 747–59 (discussing how and why police unions have been obstacles to reform); Levin, *supra* note 74, at 1340–54 (discussing two critiques of police unions, and noting that police unions "have served as a significant impediment to many reformist and transformative efforts").

77. *See* Alec Karakatsanis, *The Punishment Bureaucracy: How to Think About "Criminal Justice Reform,"* 128 YALE L.J.F. 848, 855–56 (2019) (critiquing the choices for what society criminalizes, who is targeted, and the legal rules that allow these choices to be justified).

78. *See* Stuart Schrader, *To Protect and Serve Themselves: Police in US Politics Since the 1960s*, 31 PUB. CULTURE 601, 603 (2019) ("Professionalization, moreover, conferred on police a monopoly of expertise in the particular social region of crime control. This situation created a structural trap: police gained more resources and ideological support even when they could not or did not curtail crime because officials had made campaign promises that assumed police would succeed and officials were thus loath to criticize their failures. Police gained prodigious political power in the process, touted for isolated successes and fiscally rewarded because of the mistaken belief that more resources would finally turn the tide in the fight against crime.").

government was simply unaware of police purchases.[79] This is not because they were secret but because no one really cared to be informed. As scholars Catherine Crump and Elizabeth Joh have written, procurement policies for new surveillance technology received little public notice and even less public scrutiny.[80] For decades, police departments spent their budgets as they saw fit with irregular, if any, accountability measures or community engagement. For example, in Los Angeles, police adopted systems of predictive policing, automated license plate readers, and social network analysis with almost complete autonomy.[81] In Seattle, police bought drones and a camera network without informing the local city council.[82] Recently, many police departments have experimented with facial recognition without giving notice to local elected officials.[83] Because the rules around procurement are boring and mundane, and the technology is highly technical and specialized, purchases just have not been the focus of much public interest or debate.

The trust lens has—for better or worse—been the status quo operating assumption when it comes to policing technology. In some cases, the trust is intentionally placed, deferring to police professionalism or experience. In other cases, the trust reflects a gap in oversight because no one has the capacity or competence to regulate effectively. As will be discussed in the next Section, the default to trust has produced negative outcomes, leading to abuses, mistakes, and a movement to abolish police surveillance technology.

B. RESULTS OF A TRUST-BASED APPROACH TO SURVEILLANCE

A trust-based approach to police technology resulted in a decade's worth of data-driven police surveillance mistakes. From around 2010 to 2021, the first era of big data policing seeded new surveillance technologies across the nation.[84] As will be discussed, these technologies ranged from pilot projects created by tiny

79. *See, e.g.*, Ali Winston, *Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology*, VERGE (Feb. 27, 2018, 3:25 PM), https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd [https://perma.cc/RUD9-LKPD].

80. *See generally* Crump, *supra* note 21 (discussing how law enforcement agencies obtain surveillance technologies without the knowledge of elected officials or the general public); Joh, *supra* note 21 (discussing how private surveillance technology vendors undermine the transparency of police departments).

81. *See* SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING 8–11, 41 (2021) (detailing the scope of the Los Angeles Police Department's big-data surveillance tools).

82. *See* Rubinstein, *supra* note 43, at 1987 ("The city council adopted the surveillance equipment ordinance following negative media reports and a public outcry in response to two incidents: the city's secretive acquisition of two small drones and its installation of surveillance cameras (along with a 'mesh network') at Seattle's waterfront.").

83. *See* Elizabeth Dwoskin, *Amazon Is Selling Facial Recognition to Law Enforcement - for a Fistful of Dollars*, CHI. TRIB. (May 22, 2018, 10:36 AM), https://www.chicagotribune.com/business/ct-biz-amazon-facial-recognition-program-20180522-story.html.

84. This decade timeframe is a contestable, but ultimately defensible, claim. Starting around 2010, with the rise of predictive policing, the media has accelerated an awareness of how new surveillance technologies have impacted policing. *See* Andrew Guthrie Ferguson, *High-Tech Surveillance Amplifies Police Bias and Overreach*, CONVERSATION (June 12, 2020, 8:15 AM), https://theconversation.com/

start-up ventures[85] to powerful corporate digital platforms run by billion-dollar companies.[86]

Although not representative of the full diversity of police technology, a study of Los Angeles and Chicago, two cities that have led the nation in big data surveillance, paints the picture of how technology can transform policing strategies.[87] Both cities show how a trust-based approach has led to tremendous growth in big data surveillance despite numerous mistakes, scandals, and problematic uses.

1. Los Angeles

Los Angeles, California, has led the nation in experimenting with new forms of data-driven policing.[88] In 2011, the Foothill Division of the Los Angeles Police Department (LAPD) began a double-blind study using an algorithm to see if police could predict property crimes, including burglary, car theft, and theft from automobile.[89] The simple idea was to use past crime data (calls for service of those crimes) to predict future crime patterns.[90] The underlying theory was that certain crimes have a contagion effect because of environmental vulnerabilities that encourage crime, such as poor lighting or a lack of police presence.[91] Chief William Bratton gave the greenlight to PredPol, a small start-up company leading

high-tech-surveillance-amplifies-police-bias-and-overreach-140225 [https://perma.cc/C9UE-3HLP] (discussing the recent history of big data policing).

85. *See, e.g.*, Ellen Huet, *Server and Protect: Predictive Policing Firm PredPol Promises to Map Crime Before It Happens*, FORBES (Feb. 11, 2015, 6:00 AM), https://www.forbes.com/sites/ellenhuet/2015/02/11/predpol-predictive-policing/?sh=dbad68e4f9bf.

86. *See, e.g.*, Mark Harris, *How Peter Thiel's Secretive Data Company Pushed into Policing*, WIRED (Aug. 9, 2017, 9:40 AM), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing.

87. In a series of articles and books, I have written about each of these cities and their embrace of big data policing in great detail. The summary above is necessarily limited. For more detail, see generally FERGUSON, *supra* note 6; Ferguson, *supra* note 8; and Ferguson, *supra* note 84.

88. *See* Joel Rubin, *Stopping Crime Before It Starts*, L.A. TIMES (Aug. 21, 2010, 12:00 AM), https://www.latimes.com/archives/la-xpm-2010-aug-21-la-me-predictcrime-20100427-1-story.html http.

89. *See* G. O. Mohler, M. B. Short, P. J. Brantingham, F. P. Schoenberg & G. E. Tita, *Self-Exciting Point Process Modeling of Crime*, 106 J. AM. STAT. ASS'N 100, 100, 105 (2011); *see also* Sidney Perkowitz, *Crimes of the Future: Predictive Policing Uses Algorithms to Analyse Data and Cut Crime. But Does It Really Work, and Should It Be Trusted?*, AEON (Oct. 27, 2016) https://aeon.co/essays/should-we-trust-predictive-policing-software-to-cut-crime [https://perma.cc/FBF4-S6X3] (discussing the double-blind nature of the PredPol/LAPD pilot study in Los Angeles); Justin Jouvenal, *Police Are Using Software to Predict Crime. Is It a 'Holy Grail' or Biased Against Minorities?*, WASH. POST (Nov. 17, 2016), https://www.washingtonpost.com/local/public-safety/police-are-using-software-to-predict-crime-is-it-a-holy-grail-or-biased-against-minorities/2016/11/17/525a6649-0472-440a-aae1-b283aa8e5de8_story.html (discussing the LAPD's use of PredPol in the Foothill Division).

90. *See* G. O. Mohler, M. B. Short, Sean Malinowski, Mark Johnson, G. E. Tita, Andrea L. Bertozzi & P. J. Brantingham, *Randomized Controlled Field Trials of Predictive Policing*, 110 J. AM. STAT. ASS'N 1399, 1399–400 (2015); Josh Koehn, *Algorithmic Crimefighting*, SANJOSE.COM (Feb. 22, 2012), https://www.sanjose.com/2012/02/22/sheriffs_office_fights_property_crimes_with_predictive_policing/ [https://perma.cc/47DA-LTCD].

91. *See* Huet, *supra* note 85; Rubin, *supra* note 88; Samantha Melamed, *Can Atlantic City's Bold Experiment Take Racial Bias Out of Predictive Policing?*, PHILA. INQUIRER (Aug. 10, 2017), https://www.inquirer.com/philly/news/crime/atlantic-city-risk-terrain-modeling-rutgers-predictive-policing-joel-caplan-20170810.html.

the pilot, and place-based predictive policing was born.[92] For almost a decade, PredPol shaped police patrols across greater Los Angeles.[93]

In 2011, the LAPD adopted a person-based predictive policing strategy called the Los Angeles Strategic Extraction and Restoration (LASER) program.[94] The LASER program was funded by the Smart Policing Initiative—a project of the U.S. Department of Justice's Bureau of Justice Assistance.[95] The creators callously described their goal: "The basic premise is to target with laser-like precision the violent repeat offenders and gang members who commit crimes in the specific target areas. The program is analogous to laser surgery, where a trained medical doctor uses modern technology to remove tumors or improve eyesight."[96]

The removal goal was to be effectuated by two related strategies—one focused on people and the other on places. First, the LASER program created a Chronic Offender Bulletin that identified high-risk people for additional police attention.[97] Second, the LASER program created LASER Zones, which identified high-risk places for additional police patrols.[98] Police were expected to contact identified Chronic Offenders[99] and patrol the identified zones. Chronic Offenders were labeled as such by a point system that added up criminal history and other risk

92. *Cf.* Interview by James H. Burch II & Kristina Rose with William Bratton, former Chief of Police of the L.A. Police Dep't, in L.A., Cal. (Nov. 18–20, 2009), https://bja.ojp.gov/sites/g/files/xyckuh186/files/publications/podcasts/multimedia/transcript/Transcripts_Predictive_508.pdf [https://perma.cc/CGT8-7MHH] (documenting that Chief Bill Bratton believes predictive policing allows law enforcement agencies to "gather information more quickly than ever in the past, analyze it, and from that, actually begin to predict that certain actions . . . are going to occur and seek to prevent them").

93. As will be discussed later in this Article, PredPol changed its name to Geolitica in 2021. *See Geolitica: A New Name, a New Focus*, GEOLITICA (Mar. 2, 2021), https://geolitica.com/blog/geolitica-a-new-name-a-new-focus/ [https://perma.cc/6WXE-GJGM]. Because this Article looks at retrospective facts, PredPol will be used to designate the company.

94. Brayne, *supra* note 57, at 986.

95. OFF. OF THE INSPECTOR GEN., L.A. POLICE COMM'N, REVIEW OF SELECTED LOS ANGELES POLICE DEPARTMENT DATA-DRIVEN POLICING STRATEGIES 3 (2019); CRAIG D. UCHIDA, MARC SWATT, DAVID GAMERO, JEANINE LOPEZ, ERIKA SALAZAR, ELLIOTT KING, RHONDA MAXEY, NATHAN ONG, DOUGLAS WAGNER & MICHAEL D. WHITE, BUREAU OF JUST. ASSISTANCE, DOJ, LOS ANGELES, CALIFORNIA SMART POLICING INITIATIVE: REDUCING GUN-RELATED VIOLENCE THROUGH OPERATION LASER 3 (2012).

96. UCHIDA ET AL., *supra* note 95, at 6.

97. OFF. OF THE INSPECTOR GEN., *supra* note 95, at 5 ("[T]he overall goal of the Chronic Offender Program was initially to identify persons who were committing violent crimes in a target area and to remove them from the area, presumably by arresting them. This goal appears to have evolved over time, with more recent documentation about the program suggesting engagement strategies that appear designed to deter future crime, such as by notifying identified Chronic Offenders that the police are aware of their criminal activity." (footnote omitted)).

98. *Id.* at 7 ("LASER Zones or hotspot corridors, are selected based on a historical analysis of gun-related crime data, and they are meant to be maintained for a period of at least nine months. Each LASER Zone is entered into the Palantir data analytics platform, which then allows the Department to conduct detailed tracking of crimes occurring in each zone as well as the amount of time officers spend there.").

99. *Id.* at 5 ("Once a Chronic Offender is selected, using pre-determined criteria, a Chronic Offender Bulletin is generated and disseminated to field personnel. These bulletins are intended to 'assist officers in identifying crime trends and solving current investigations, and to give officers a tool for proactive police work (e.g., a list of offenders to proactively seek out).'").

factors.[100] Patrol strategies, thus, evolved to contact targeted individuals both as a measure of social surveillance and data collection, which was inputted into the LAPD's digital investigative platform run by a private company, Palantir.[101] Palantir has a multimillion dollar contract to assist LAPD in keeping track of the various crime patterns in the city.[102] As Professor Sarah Brayne has revealed in her book on the Palantir–LAPD partnership, the goal was to collect as much data as possible on criminal groups for possible intervention and investigative purposes.[103]

Augmenting these types of place-based, person-based, and group-based predictive technologies were more traditional surveillance technologies. LAPD invested in drones, automated license plate readers, facial recognition pilots, and a host of digital tracking technologies.[104] In addition, legacy databases, such as

---

100. *Id.* at 6. The Chronic Offender Program's point system has changed since the program was first implemented. Specifically,

> At the inception of the program, each person who was the subject of a work-up received the following:
>
> - 5 points if the individual is a gang member.
> - 5 points if the individual is on parole or probation.
> - 5 points if the individual had any prior arrests with a handgun.
> - 5 points if the individual had any violent crimes on his or her rap sheet.
> - 1 point for every "quality police contact" in the last two years.
>
> In 2017, two criteria in the point system above were modified to include the following considerations:
>
> - Identify the number of violent crime arrests the individual had over the last two years. Apply 5 points for each violent crime arrest.
> - Determine whether the individual has used a gun in the course of his/her activities. Apply 5 points for each incident involving a gun over the last two years.

Id. (footnote omitted).

101. *See id.* at 7 ("Based on Department materials provided to the OIG, the Department's recommended follow-up activities included: 1) sending a letter to the offender; 2) conducting warrant checks; 3) conducting parole/probation compliance checks; and 4) conducting door knocks and advising the offender of available programs and services designed to reduce the risk of recidivism. Personnel who are assigned an offender are to provide a status update to their Commanding Officer every two weeks regarding what actions have been taken with that offender. This information is also entered into a database."); *see also* Matt Burns, *Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients*, TECHCRUNCH (Jan. 11, 2015, 7:37 PM), http://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/ [https://perma.cc/3MTJ-5J2N] ("Detectives love the type of information it [Palantir] provides. They can now do things that we could not do before. They can now exactly see great information and the links between events and people." (alteration in original)).

102. *See* Harris, *supra* note 86.

103. *See* BRAYNE, *supra* note 81, at 37–45.

104. *See* Henry Kenyon, *California Police Are Lax in Securing License Plate Data, Audit Finds*, CQ ROLL CALL (Feb. 24, 2020), 2020 WL 880515 (automated license plate readers); Kate Mather, *LAPD Becomes Nation's Largest Police Department to Test Drones After Oversight Panel Signs Off on Controversial Program*, L.A. TIMES (Oct. 17, 2017, 9:05 PM), http://www.latimes.com/local/lanow/la-me-ln-lapd-drones-20171017-story.html (drones); Kevin Rector, *LAPD Panel Approves New Oversight of Facial Recognition, Rejects Calls to End Program*, L.A. TIMES, (Jan. 12, 2021, 4:00 PM), https://www.latimes.com/california/story/2021-01-12/lapd-panel-approves-new-oversight-of-facial-recognition-rejects-calls-to-end-program (facial recognition).

CalGang, and federal fusion centers rounded out the growing data-driven power of police.[105]

At no point in the development of predictive policing, Palantir's platform, or other surveillance technologies were any significant legislative or judicial limits imposed. Police innovated and were mostly left alone because of a default to trust. While advocates complained about the growing systems of surveillance,[106] police were given free rein to adopt new technologies without significant public accountability or transparency.

2. Chicago

Running a close second to Los Angeles, Chicago also invested heavily in big data surveillance.[107] The Chicago Police Department developed strategies around predictive policing, surveillance cameras, sensors, social media surveillance, and video analytics[108]—all without significant regulation or legislative authorization.

Chicago was one of the first cities to experiment with a person-based predictive policing strategy called the Strategic Subjects List (colloquially known as the Heat List).[109] Inspired by sociologists who advocated for a public health approach to violence, Chicago started identifying individuals it believed were most likely to be perpetrators or victims of violent crime.[110] Employing an algorithm invented by academics at the Illinois Institute of Technology, the police began rank ordering "at risk" individuals with the goal of guiding police intervention toward these higher risk people.[111] The inputs for the algorithm—what became

105. *See* CAL. STATE AUDITOR, THE CALGANG CRIMINAL INTELLIGENCE SYSTEM: AS THE RESULT OF ITS WEAK OVERSIGHT STRUCTURE, IT CONTAINS QUESTIONABLE INFORMATION THAT MAY VIOLATE INDIVIDUALS' PRIVACY RIGHTS, REPORT 2015-130, at 1 (2016), https://auditor.ca.gov/pdfs/reports/2015-130.pdf [https://perma.cc/R97M-F4EJ] (explaining that CalGang is a shared criminal intelligence system that allows law enforcement officers to enter information on suspected gang members); *see also* Petra Bartosiewicz, *Beyond the Broken Window: William Bratton and the New Police State*, HARPER'S MAG. (May 2015), https://harpers.org/archive/2015/05/beyond-the-broken-window/ ("The LAPD, for example, retains all [Suspicious Activity Reports], even those that prove unfounded, for at least one year, and shares them with the local fusion center, which keeps them for up to five.").

106. *See, e.g.*, STOP LAPD SPYING COAL., BEFORE THE BULLET HITS THE BODY: DISMANTLING PREDICTIVE POLICING IN LOS ANGELES 5, 29–31 (2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf [https://perma.cc/A3ME-ZVJZ].

107. *See* Mark Guarino, *Can Math Stop Murder?: In Besieged Chicago, How Police Are Tapping Big Data to Try to Curb Gang Violence*, CHRISTIAN SCI. MONITOR (July 20, 2014), https://www.csmonitor.com/USA/2014/0720/Can-math-stop-murder.

108. *See* HOLLYWOOD ET AL., *supra* note 56, at 9–13.

109. *See* Jeremy Gorner, *Chicago Police Use 'Heat List' as Strategy to Prevent Violence*, CHI. TRIB. (Aug. 21, 2013), http://www.chicagotribune.com/news/ct-xpm-2013-08-21-ct-met-heat-list-20130821-story.html. The Strategic Subjects List is also known as the Crime and Victimization Risk Model (CVRM). The name change corresponded with negative publicity about the use of person-based predictive policing technologies. *See* HOLLYWOOD ET AL., *supra* note 56, at 12 ("The Crime and Victimization Risk Model (CVRM) is a revision of the earlier Strategic Subject List (SSL) tool that assessed the risk that a person would be a party to gun violence (either as a victim or perpetrator).").

110. *See* Andrew V. Papachristos & David S. Kirk, *Changing the Street Dynamic: Evaluating Chicago's Group Violence Reduction Strategy*, 14 CRIMINOLOGY & PUB. POL'Y 525, 533 (2015).

111. *See* Andrew Guthrie Ferguson, *The Police Are Using Computer Algorithms to Tell if You're a Threat*, TIME (Oct. 3, 2017, 11:29 AM), https://time.com/4966125/police-departments-algorithms-chicago/; Nissa Rhee, *Can Police Big Data Stop Chicago's Spike in Crime?*, CHRISTIAN SCI. MONITOR

known as the Heat List—changed over time but included arrests for narcotics, arrests for weapons offenses, arrests for assaults, being assaulted oneself, age, and (in earlier iterations) gang membership.[112] The list initially predicted 400 high-risk targets for police intervention, but the list eventually grew to over 300,000 individuals.[113] Interventions included home visits by police, custom notification letters detailing why these individuals were at risk, and greater street surveillance.[114] Until the program was shut down, almost everyone arrested in Chicago was given a numerical, predictive threat score (with scores ranging from zero through over 500) based on this risk index.[115]

Chicago also adopted a place-based, predictive patrol management system with Hunchlab.[116] This partnership involved a similar predictive policing strategy that directed patrol units to identified higher risk areas. Hunchlab's algorithm used inputs for risk that included crime, date, location, weather, days of the week, and other environmental factors.[117] In 2018, Hunchlab was acquired by ShotSpotter, a gunshot detection system also utilized by Chicago police to identify the location of gunshots for police investigation.[118]

Most controversially, Chicago invested in over 30,000 networked video cameras connected to local control centers called Strategic Decision Support Centers (SDSCs).[119] These command centers aggregated numerous different surveillance technologies.[120] Information flowing to these command centers include automated license plate readers, social network analysis charts, and information about

(June 2, 2016), https://www.csmonitor.com/USA/Justice/2016/0602/Can-police-big-data-stop-Chicago-s-spike-in-crime.

112. *See* Mick Dumke & Frank Main, *A Look Inside the Watch List Chicago Police Fought to Keep Secret*, CHI. SUN-TIMES (May 18, 2017, 9:26 AM), https://chicago.suntimes.com/news/what-gets-people-on-watch-list-chicago-police-fought-to-keep-secret-watchdogs.

113. *See* Ferguson, *supra* note 111; HOLLYWOOD ET AL., *supra* note 56, at 12.

114. *See* Ferguson, *supra* note 111.

115. *See id*.

116. Timothy Mclaughlin, *As Shootings Soar, Chicago Police Use Technology to Predict Crime*, REUTERS (Aug. 5, 2017, 6:25 AM), http://www.reuters.com/article/us-chicago-police-technology/as-shootings-soar-chicago-police-use-technology-to-predict-crime-idUSKBN1AL08P [https://perma.cc/9937-9HX8]; *see also* AZAVEA, HUNCHLAB: UNDER THE HOOD 5 (2015), http://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf [https://perma.cc/BM8Y-EP7X] (providing history on Hunchlab).

117. AZAVEA, *supra* note 116, at 10.

118. *See* HOLLYWOOD ET AL., *supra* note 56, at 10 (ShotSpotter has been running a risk analytics program called ShotSpotter Missions that builds off of Hunchlab's technology); Andrew Westrope, *Gunshot Detection Company ShotSpotter Acquires Predictive Policing Software*, GOV'T TECH. (Oct. 15, 2018), https://www.govtech.com/biz/Gunshot-Detection-Company-ShotSpotter-Acquires-Predictive-Policing-Software.html [https://perma.cc/N3KX-28YU].

119. *See* HOLLYWOOD ET AL., *supra* note 56, at 8–9 (detailing the network of 35,000 cameras); *see also* Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html.

120. *See* HOLLYWOOD ET AL., *supra* note 56, at 8 ("These centers include predictive crime software that helps district leadership make deployment decisions, additional cameras, gunshot detection systems, and mobile phones to officers in the field who receive real-time notifications and intelligence data at their fingertips.").

suspects from police databases.[121] Digital video cameras with analytic capabilities watch entire neighborhoods.[122] These video feeds are analyzed along with crime data and human intelligence in an effort to identify the crime drivers in an area.[123]

Despite complaints about predictive policing and a growing realization that the Heat List was racially biased and flawed,[124] Chicago Police have embraced data-driven policing without serious oversight or accountability mechanisms. Fueled by philanthropic donations and federal grants, police technology is now front and center of Chicago's future.[125]

C. WHY TRUST IS INADEQUATE

A trust-based police surveillance lens should be resisted for one simple reason: it has failed in practice. The precise argument here is that the trust-based approach—not the policing technologies—has failed, but the series of reversals and mistakes may well suggest a broader failure that includes both the approach and the underlying technologies.

As to actual practice, both cities discussed above have had to walk back or reject their use of the technologies touted as the "next new thing" to fight crime. Beginning with Los Angeles, the LAPD canceled its contract with PredPol in 2020.[126] Although the LAPD cited budget cuts as the reason it would stop using

---

121. *Id.* at 9–13 ("The CPD has developed a social network analysis tool that displays, for a given subject, the first- and second-degree co-arrest links around them. This tool also permits drill-downs on selected subjects, bringing up criminal history information about them.").

122. *Id.* at 34 ("They have been granted access to a system to run automated analytics on video that supports keyword searching for specific types of features and events, but they are often limited by usage quotas and the required bandwidth to transfer video into the analytic system.").

123. *Id.* (noting that applications included (1) "conducting virtual surveillance missions, looking for suspicious activity in progress," (2) "providing near–real-time surveillance of a reported crime scene, identifying perpetrators, victims, and potential witnesses," (3) "providing overwatch support to units responding to a crime scene, helping officers deploy to scene effectively and safely," and (4) "looking for suspects and their vehicles fleeing a crime scene").

124. *See* Brianna Posadas, *How Strategic Is Chicago's "Strategic Subjects List"? Upturn Investigates.*, MEDIUM (June 22, 2017), https://medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c [https://perma.cc/954F-YVQ3].

125. *See, e.g.*, Bryan Llenas, *Brave New World of 'Predictive Policing' Raises Specter of High-Tech Racial Profiling*, FOX NEWS (Jan. 11, 2017), http://latino.foxnews.com/latino/news/2014/02/24/brave-new-world-predictive-policing-raises-specter-high-tech-racial-profiling/ [http://perma.cc/VG5W-WV93] ("[T]he Chicago Police Department, thanks to federal funding, is now helping to drive policing into territory previously only dreamed of in science fiction: The ability to essentially predict who will be the next perpetrator or the next victim of a crime."); Craig Wall, *Chicago Given $10M to Expand Predictive Policing, Officer Training*, ABC 7 CHI. (Apr. 11, 2018), https://abc7chicago.com/chicago-given-$10m-to-expand-predictive-policing-officer-training/3327651/ [https://perma.cc/B62D-CDKC] ("Chicago police are getting a $10 million dollar [sic] donation to help with crime fighting technology.").

126. *See* Caroline Haskins, *The Los Angeles Police Department Says It Is Dumping a Controversial Predictive Policing Tool*, BUZZFEED NEWS (Apr. 21, 2020, 7:34 PM), https://www.buzzfeednews.com/article/carolinehaskins1/los-angeles-police-department-dumping-predpol-predictive [https://perma.cc/4FSH-Q3PJ].

the software, the real reasons were community pressure and a lack of evidence that the predictive policing system had any meaningful impact on crime rates.[127]

Similarly, a devastating Inspector General's audit of the LAPD LASER program demonstrated that the system was flawed in numerous ways.[128] The Inspector General's investigation was the direct result of community activists who protested, petitioned, and exposed the problems in the program.[129] This was not so much an example of police checking themselves as much as the community forcing their hand. The Inspector General's audit of the LASER program revealed how trust was an insufficient check on police power. Among other things, the audit found that the LASER program encouraged unconstitutional stops,[130] had few rules,[131] no training protocols,[132] and reified existing racial disparities.[133] Most troublingly, the data-driven point system based on arrests, contacts, and criminal history was being applied haphazardly. Some high-priority targets on the LASER list had no points from the system,[134] forty-four percent had only one or zero arrests,[135] and nearly ten percent of Chronic Offenders did

127. *See id.* An internal agency audit found that the LAPD "struggled to measure PredPol's effect on crime — or prove that it works." *Id.*

128. *See generally* OFF. OF THE INSPECTOR GEN., *supra* note 95 (analyzing the LASER program, identifying "significant barriers" and concerns, and proposing recommendations).

129. *See* Eva Ruth Moravec, *Do Algorithms Have a Place in Policing?: How a Pakistani-Born Retired Pilot Took on a Controversial, Data-Driven Policing Program in Los Angeles—and Won*, ATLANTIC (Sept. 5, 2019), https://www.theatlantic.com/politics/archive/2019/09/do-algorithms-have-place-policing/596851/.

130. *See* OFF. OF THE INSPECTOR GEN., *supra* note 95, at 11 ("[T]he language related to making stops of Chronic Offenders lacked precision. After suggesting that officers who see designated Chronic Offenders 'may stop them, do a field interview, and let them go, if appropriate,' the document also states that '[i]n many situations, however, as with all stops, [the stops] should be constitutional and legal.'" (second and third alterations in original)).

131. *See id.* at 12.

132. *See id.* ("The OIG found that training practices related to Operation LASER also appeared, in many cases, to be informal.").

133. *See id.* at 15.

134. *See id.* ("[I]t appeared that some Areas were not assigning points at all when selecting offenders, relying instead on referrals from detectives or patrol personnel. Apparently as a result, 37 people listed as 'Active,' as well as 75 people listed as 'Inactive,' were added to the database with a total of zero points.").

135. *Id.* at 16. The report found:

> Due to the Chronic Offender Program's focus on individuals who are most actively involved in violent and/or gun-related crime, the OIG also reviewed the points assigned for these categories, where available, and found the following:
>
> - While some Chronic Offenders were listed as having a large number of arrests for violent crimes, nearly half — 44 percent — of those with detailed point calculations were listed as having either zero or one such arrest.
> - While about half of Chronic Offenders were listed as having one or more reported arrests for gun-related crimes, about half were listed as having no such arrests.

Id. (footnote omitted).

not have any "quality police contacts" registered in the system.[136] The information was also rarely updated or double checked.[137] In 2020, the LAPD shut down the LASER program completely.[138]

Chicago also cancelled its once touted Strategic Subjects List after the RAND Corporation conducted an audit and revealed its flaws.[139] RAND undertook a complete review of the big data technologies used by the Chicago Police Department and found, among other things, that person-based predictive policing in the form of the Strategic Subjects List (and second-generation versions) were neither effective nor accurate.[140]

Two significant problems surfaced. First, the models identifying at-risk individuals were overbroad. Even in the best-case scenario, the model forecasted risk eighteen months out and included over 10,000 high-risk people and hundreds of thousands of others with risk scores.[141] Targeted intervention models need to respond quickly, and identifying risk over a year and a half time frame did not help police reduce risk on a daily basis.[142] In addition, the 10,000 number, while a small percentage of Chicago residents, was too large for police to target effectively. Second, and relatedly, the risk-identification system did not offer any suggested intervention strategies.[143] So even an accurate and timely list of 10,000 people did not provide police with any actionable information to reduce crime (except a target list).[144] In short, people were being identified, but there was no strategy or follow-through to reduce the risk of violence.[145]

Additionally, the inputs used—arrests—were too easily influenced by police action, leading the identification process to be infected by selection bias and

136. *Id.* ("Nearly 10 percent of the Chronic Offenders in the database did not have any 'quality police contacts' recorded, and the majority had less than five such contacts. Alternatively, several Chronic Offenders were listed as having been contacted by the police anywhere from 20 to 45 times.").

137. *See id.* at 17–18.

138. *See* Haskins, *supra* note 126.

139. *See* HOLLYWOOD ET AL., *supra* note 56, at 36–38; Sam Charles, *CPD Decommissions 'Strategic Subjects List*,' CHI. SUN-TIMES (Jan. 27, 2020), https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson.

140. *See* HOLLYWOOD ET AL., *supra* note 56, at 36–38.

141. *See id.* at 36, 38 ("The CVRM or SSL provides risk scores for everyone arrested in Chicago at some point over the past four to five years, which constitutes hundreds of thousands of people. As noted above, only a few thousand had high-risk labels, with the remaining several hundred thousand largely discounted from further consideration.").

142. *See id.* at 36 ("[T]he full process (administrative and technical) of running the model takes several months, and has taken up to years, to come up with updated data sets. This pace is in contrast with the commonly held perspective that the real-world risks of violence can escalate very quickly, and the CPD must be able to diagnose and respond quickly.").

143. *See id.* at 35 ("[T]he CPD did not identify a specific intervention to take action directly on those whom the model flagged as being in the high-risk bands.").

144. *See id.* at 37 ("The CVRM input data can provide some insight into what services and other interventions a person might need, but really understanding a person's needs would require information outside traditional police records management systems. This information includes human intelligence, social service, educational, and even medical and (especially) mental health records and diagnostics.").

145. *See id.* at 35–38.

personal discretion.[146] As I have previously written, the use of police-influenced inputs, such as arrests or contacts, necessarily distorts the risk analysis because police are developing suspicion through their own actions independent of the targeted person's actions.[147] Essentially, police are predicting their own future arrest patterns based on past policing patterns.

While Chicago's predictive policing systems have ended, other big data surveillance systems continue to guide strategy with little more than trust as oversight. As discussed earlier, localized SDSCs fueled by video and analytics have supercharged the same type of targeted surveillance.[148] Growing digital camera networks show no signs of shrinking or of being regulated.[149] Audio sensors and place-based predictive policing are still used in the city. Real-time surveillance and response are becoming the norm. In fact, the same RAND report that critiqued predictive policing validated Chicago's embrace of other big data surveillance technologies.[150] Even in the face of documented failure, trust remains the dominant approach.

D. CONCLUSION ON THE TRUST LENS

Los Angeles and Chicago show the impact of relying on a trust-based approach to new technologies. A general deference to police power was combined with the increased deference to policing technology, and the result was predictably harmful to those policed. Until advocates and journalists started exposing the flaws in the predictive systems, police embraced them and used them without much second thought. Despite clear problems reflecting structural biases, the technologies increased police power, redirected surveillance against minority communities, and generated significant community concern.

The above examples in Los Angeles and Chicago were not simply failures of technology but failures of vision. The focus on data collection and data analysis came with a blindness to a host of social, economic, and racial issues that are problematic to surveillance. As I have written about before, predictive policing

146. *See* FERGUSON, *supra* note 6, at 75 ("Predictive systems based primarily on arrests will mirror policing more than predictive systems focused on reported crimes will.").

147. *See* Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 OHIO ST. J. CRIM. L. 503, 515 (2018) ("[P]erson-based predictive models may result in seemingly racially discriminatory effects. For example, if the algorithm that identifies people on the [H]eat [L]ist includes information about prior arrests, or connections with people who are arrested, then where police are looking for arrests will impact the resulting risk identification system.").

148. *See supra* note 119 and accompanying text.

149. *See Chicago Police Launch Their Latest 'Nerve Center' in Bid to Fight Crime with High-Tech Tools*, CBS CHI. (June 25, 2020, 1:23 PM), https://chicago.cbslocal.com/2020/06/25/chicago-police-launch-their-latest-nerve-center-in-bid-to-fight-crime-with-high-tech-tools/ [https://perma.cc/P2P9-S6CK] (noting that Chicago has expanded its use of technology to reduce crime and SDSCs are in place in twenty-one of Chicago's twenty-two police districts).

150. *See* HOLLYWOOD ET AL., *supra* note 56, at 46–48. The RAND report on Chicago's Real Time Crime Centers offers a counterpoint to the critiques of big data technologies. The RAND report details the utility of centralized data sources, linked camera systems, and ever-increasing data aggregation. *Id.* at 25–27. For investigators, unconcerned with implications of privacy and security, the additional information and ease of access allows a powerful new tool to investigate crimes.

systems failed to address problems of data error, methodology, security, transparency, accountability, and vision.[151] In addition, the surveillance systems failed to account for concerns about race, transparency, unequal data sources, and a host of other constitutional problems.[152]

Equally concerning, the growth of big data policing led to a concentration of surveillance on the poorest communities and communities of color. In Los Angeles and Chicago, most individuals caught in the lens of surveillance are Black and brown, young and poor.[153] Patterns of systemic overenforcement in historically minority communities were replicated in the deployment of surveillance cameras and algorithmically nudged patrols.[154] All big data policing is encoded with race, and so the same "black data" problems that exist in policing were mirrored in the adoption of police surveillance systems.[155]

The takeaway from this list of setbacks and systemic failures is that trusting the police to develop and implement surveillance technology without oversight, accountability, or checks may be unwise. Independent of the merits of the technology, the lack of oversight and the default to trust have failed in practice. And, on the merits, the use of new policing technologies may be dangerous to certain communities. As discussed in the next Part, the rapid growth and deployment of big data policing technologies quickly created a movement to ban them.

II. THE TRAP LENS

Policing has never been without its critics. Concerns about tactics, bias, and systemic patterns of oppression have followed the institution of policing since its creation.[156] This criticism has grown louder with the increased power of surveillance technology, and louder still after the murder of George Floyd and the national reckoning with systemic police racism.[157] Policing has been challenged

151. *See* Ferguson, *supra* note 8, at 1180–84 (discussing problems of vision).

152. *See* Ferguson, *supra* note 147, at 504 (detailing the argument that all big data policing has a "black data" problem, involving race, transparency, and constitutional distortion). "[B]ig data policing technologies must address this lack of transparency, the legacy of racial discrimination, and the constitutional uncertainty arising from application in the real world." *Id.*

153. *Cf.* Alisa Tiwari, *Disparate-Impact Liability for Policing*, 129 YALE L.J. 252, 267 (2019) ("Excessive enforcement and surveillance practices fuel mass incarceration and the accumulation of criminal records in minority neighborhoods."). For a discussion of the disproportionate percentage of young men of color under police surveillance, including on the Chicago and Los Angeles predictive policing lists, see *infra* notes 170–74 and accompanying text.

154. *See* Bedoya, *supra* note 25; Roberts & Vagle, *supra* note 25.

155. *See* Ferguson, *supra* note 147, at 504 (discussing race and big data policing).

156. *See infra* Section II.A.

157. *See* Aaron Ross Coleman, *Minneapolis May Be the First City to Dismantle the Police*, VOX (June 8, 2020, 3:30 PM), https://www.vox.com/2020/6/8/21283980/minneapolis-defund-the-police-george-floyd-black-lives-matter. *See generally* Derek Thompson, *Unbundle the Police: American Policing Is a Gnarl of Overlapping Services That Should Be Demilitarized and Disentangled*, ATLANTIC (June 11, 2020), https://www.theatlantic.com/ideas/archive/2020/06/unbundle-police/612913/ (commenting that "[m]odern law enforcement has become a gnarl of unnecessary violence and heavily armed street counseling," and proposing that disentangling police functions could make cities safer).

as being the problem. Calls to abolish the police or defund the police have redirected the national conversation in radical and powerful ways.[158] As part of that conversation, surveillance technology—as a mechanism of social control—has been seen as another oppressive tool of police power.[159] Critics maintain that any additional technology, even if adopted for benign reasons, will eventually be used against the groups that have historically seen the blunt end of police brutality, abuse, and carceral control.[160]

A. WHY SURVEILLANCE IS A TRAP

The easiest way to distill the trap lens critique is to ask a simple question: has there ever been a time when police power was not turned against Black, brown, minority, and poor citizens in an effort to exert social control? Because the historical answer is no,[161] the trust lens holds little purchase.

Historians have cataloged how policing in general and surveillance in particular have been deployed against freed slaves, poor workers, civil rights activists, and dissenting voices in American history.[162] In the North and South—and in every century throughout American history—the law justified unequal treatment against African-American citizens via lawful police force.[163] Almost every era

158. *See* Amna A. Akbar, *Demands for a Democratic Political Economy*, 134 HARV. L. REV. F. 90, 106–12 (2020) (discussing the movement to defund the police).

159. *See* Devich-Cyril, *supra* note 17.

160. *See, e.g.*, Khan & White, *supra* note 18.

161. *See* M Adams & Max Rameau, *Black Community Control over Police*, 2016 WIS. L. REV. 515, 527 ("The specific system of power used to enforce the economic and social relationship between low-income Black communities in the United States and the larger White community in general, and corporate interests in particular, is the domestic colony. In the context of the domestic colony, the police are responsible for maintaining the coercive exploitative and oppressive relationship by serving as an occupying force in low-income Black communities."); Dorothy E. Roberts, *The Supreme Court 2018 Term—Foreword: Abolition Constitutionalism*, 133 HARV. L. REV. 1, 26 (2019) ("Police normally treat residents in communities of color in an aggressive fashion — shouting commands, handcuffing even children, throwing people to the ground, and tasing, beating, and kicking them. For young men of color, the risk of being killed by the police is shockingly high and police use of force is among the leading causes of death. Black women, women of color, and queer women are especially vulnerable to gendered forms of sexual violence at the hands of police." (footnotes omitted)).

162. *See* SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 12–17 (2015); VITALE, *supra* note 24, at 46–47; I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1288–89 (2017); Larry Redmond, *Why We Need Community Control of the Police*, 21 LOY. PUB. INT. L. REP. 226, 227 (2016) ("After the Civil War, and because income inequality was rapidly increasing, the economic elite began using police department personnel to break strikes and quell protests against worker oppression. Social control became defined as crime control by isolating 'dangerous classes' as the embodiment of the crime problem. These 'dangerous classes' consisted mainly of immigrants and free blacks." (footnotes omitted)).

163. *See* Redmond, *supra* note 162, at 226 ("In the 1700s, watchmen in northern states and slave catchers in southern states were the genesis of modern police departments."); Roberts, *supra* note 161, at 20–21 ("Beginning in the early 1700s, southern white men formed armed groups that entered slaveholding properties and roamed public roads to ensure that enslaved people did not escape or rebel against their enslavers. Slave patrols monitored enslaved people to prevent them from engaging in forbidden activities such as 'harboring weapons or fugitives, conducting meetings, or learning to read or write.'" (footnote omitted) (quoting VITALE, *supra* note 24, at 46)); *id.* at 21 ("Modern police forces are descendants of armed urban patrols like the Charleston City Guard and Watch, which was established as early as 1783 to constantly monitor and inspect both enslaved and free black residents to 'minimize

has required formal commissions to investigate systemic police misconduct.[164] Yet, the problems remain and run deep within structural levers in society. Thousands of people have been killed and millions traumatized by lawful (and unlawful) police force.[165] Millions more people are routinely processed through misdemeanor courts, hit with fines and fees for violations, and stopped in humiliating police encounters.[166] Even more have become accustomed to sacrificing liberty under the guise of lawful surveillance.

This Section details the trap lens' concerns. The argument against police surveillance technologies begins with the argument against police.[167] The trap lens echoes abolitionists' concerns that seek to dismantle prisons, policing, and the larger carceral power structure.[168] The trap lens, like the abolitionist movement, starts with the premise that the institution of policing is anti-Black, with a history and practice of valuing the economic and property interests of white citizens at

---

Negro fraternizing and, more especially, to prevent the growth of an organized colored community.'" (quoting VITALE, *supra* note 24, at 47)); Seth W. Stoughton, *The Blurred Blue Line: Reform in an Era of Public & Private Policing*, 44 AM. J. CRIM. L. 117, 123 (2017) ("In the American South, an economy heavily dependent on slavery gave rise to a different set of institutions that shared some of the responsibility for policing functions."); *id.* at 124 (Southern anxieties about slave revolt were not limited to rural plantations. Early on, cities and towns' 'enforcement [was] entrusted to private individuals and the existing watch,' but soon the model of the rural slave patrol was adopted in the form of city guards." (alteration in original) (quoting KRISTIAN WILLIAMS, OUR ENEMIES IN BLUE: POLICE AND POWER IN AMERICA 41 (2007))).

164. *See* Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054, 2069 (2017) ("A high watermark was the 1968 Kerner Commission Report, commissioned by the Johnson Administration in the wake of twenty-three episodes of urban unrest during the mid- and late 1960s. The Report concluded that, for many African Americans, the 'police have come to symbolize white power, white racism, and white repression.'" (footnote omitted) (quoting NAT'L ADVISORY COMM'N ON CIV. DISORDERS, REPORT OF THE NATIONAL ADVISORY COMMISSION ON CIVIL DISORDERS 5 (1968), https://belonging.berkeley.edu/sites/default/files/kerner_commission_full_report.pdf?file=1&force=1 [https://perma.cc/VGG3-7MP7])); *see also* Redmond, *supra* note 162, at 228 ("Over the years, various attempts, including commissions, have been made to control the abuses perpetrated by the police. However, none of them have worked. Commissions inform the public, but they have little lasting impact on police practices." (footnote omitted)).

165. *See* Moran, *supra* note 35, at 993 ("Whether wittingly or not, the legal system's deeply-ingrained deference to police officers has, for decades, effectively rubberstamped the widespread mistreatment of minorities, and allowed police departments to turn a blind eye to abuses by their own officers."). *See generally* BUTLER, *supra* note 24 (discussing how the criminal justice system is institutionally construed to watch and control Black men); POLICING THE BLACK MAN: ARREST, PROSECUTION, AND IMPRISONMENT (Angela J. Davis ed., 2017) (exploring the critical issues of race and justice in America, and critiquing how the criminal justice system affects Black boys and men at every stage of the criminal process, from arrest through sentencing).

166. Issa Kohler-Hausmann, *Managerial Justice and Mass Misdemeanors*, 66 STAN. L. REV. 611, 629–32 (2014); Alexandra Natapoff, *Misdemeanors*, 85 S. CAL. L. REV. 1313, 1315 (2012).

167. *See generally* Keeanga-Yamahtta Taylor, *The Emerging Movement for Police and Prison Abolition*, NEW YORKER (May 7, 2021), https://www.newyorker.com/news/our-columnists/the-emerging-movement-for-police-and-prison-abolition (discussing police reform, and noting that police and prisons are not solving problems related to crime and violence but instead "are a part of the problem").

168. I do not presume to speak for abolitionists and have used the trap lens terminology to create a related but different conception of a philosophy deeply skeptical of police surveillance technology. The trap lens is shorthand for those who believe that surveillance is a trap to ensnare the poor and, more specifically, communities of color.

the expense of everyone else.[169] Examining the deployment of surveillance technologies confirms the suspicions of an unequal focus on Black, brown, and poor communities in order to benefit those with existing social and economic capital.[170] As discussed, the individuals on Chicago's Heat List were primarily Black men.[171] At its height, more than half the Black men ages twenty to twenty-nine years old in Chicago were on the list.[172] Similarly, in Los Angeles, most of the men targeted through the LASER program were Black and Latino.[173] Because these policies were designed to direct police attention toward one group and away from other groups, it matters that the groups chosen for surveillance are Black and brown. By adopting predictive policing models with racially biased inputs, one necessarily adopts the recommendations that can create racially biased outputs. Similar concerns have long been raised about gang databases, which also collect more data about young men of color than other populations.[174]

These examples show how modern policing technologies have not escaped the critique leveled for centuries about discriminatory policing. The systems are technologically biased in design because the people who use and create the technology are enmeshed in social contexts that are racially biased. Surveillance, like policing, is structurally unequal, leading to legitimate claims of racial bias and a fear that any enhancement of that power is a trap to be used against those with less power.

B. THE RESULTS OF THE TRAP LENS

To look at this consistent pattern of anti-Black, opaque, and inherently biased policing history with clear-eyed sight is to see the trap ahead with policing

169. *See* Amna A. Akbar, *Toward a Radical Imagination of Law*, 93 N.Y.U. L. REV. 405, 449–50 (2018) ("Over time, police have been central to the agenda of racial capitalism and the devaluation of Black life. The rise of mass incarceration, overcriminalization, and zero-tolerance or broken windows policing is seen as an evolution of the regime of control, exclusion, and exploitation that began with slavery, convict leasing, the Black Codes, and segregation."); *see also* Bell, *supra* note 164, at 2071 ("A large body of historical research has documented the entanglement of police in the long-running national project of racial control.").

170. *See, e.g.*, Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html; J. Cavanaugh Simpson, *Prying Eyes: Military-Grade Surveillance Keeps Watch over Baltimore and City Protests, but Catches Few Criminals*, BALTIMORE (Aug. 5, 2020, 1:08 PM), https://www.baltimoremagazine.com/section/community/surveillance-planes-watch-over-baltimore-but-catch-few-criminals/ [https://perma.cc/D8TW-LQVF].

171. *See* Dumke & Main, *supra* note 112 ("[T]he vast majority of people with the highest score — 85 percent — were African-American men.").

172. Yana Kunichoff & Patrick Sier, *The Contradictions of Chicago Police's Secretive List*, CHICAGO (Aug. 21, 2017, 8:44 AM), http://www.chicagomag.com/city-life/August-2017/Chicago-Police-Strategic-Subject-List/ [https://perma.cc/2PDQ-53FW] (detailing how fifty-six percent of African-American men ages twenty to twenty-nine received a police Strategic Subjects List score).

173. *See* OFF. OF THE INSPECTOR GEN., *supra* note 95, at 15 (documenting that eighty percent of the men listed as chronic offenders were Latino and African-American).

174. *See, e.g.*, Larry Smith, *Former Baltimore Police Officer Criticizes the Department's Gang Database*, APPEAL (July 23, 2018), https://theappeal.org/former-baltimore-police-officer-unloads-on-departments-gang-database/ [https://perma.cc/2UGX-QR4A].

technology. Surveillance, the argument goes, will never be used as anything other than a tool for oppressing those with less political, cultural, and economic power.[175] For this reason, many advocates have pushed for an absolute ban on new police technology. Early targets have involved predictive policing and facial recognition technology (with some local success).[176]

As a first-principles argument, the trap lens toggles between a rhetorical push to ban all surveillance technologies and an acknowledgment that community control may be a second-best alternative. This Section examines the logic of the more extreme position, saving a more moderate response for the next Sections. Those who favor the former approach—surveillance abolitionists—argue that any regulation short of a full ban legitimatizes illegitimate power.[177] In other words, a true trap mentality recognizes the need for a full ban as a first-principles starting (and ending) point. In recent years, trap lens advocates can point to three clear victories from this approach: public mobilization, corporate moratoriums, and the development of a theoretical framework to abolish police surveillance technology.

1. Public Mobilization

The trap lens has been an effective mobilizing tool to rally communities against encroaching police technology.[178] Even before the murder of George Floyd, the fear of surveillance provided community activists with a clear target for complaint.[179] In many ways, police surveillance technologies offered a proxy attack on policing in general. For example, while defunding an entire police department might be difficult for political or policy reasons, dropping a particular vendor or predictive software program is much easier. As a matter of community sentiment and protest organizing, rallying against surveillance created a new movement against police power.

This grassroots organizing had real impact. Community leaders in Detroit, New York City, and other cities across the nation challenged particular technologies such as facial recognition.[180] In the heart of Silicon Valley, the American

175. *See* Khan & White, *supra* note 18.

176. *See, e.g.*, Avi Asher-Schapiro, *California City Bans Predictive Policing in U.S. First*, REUTERS (June 24, 2020, 2:33 PM), https://www.reuters.com/article/us-usa-police-tech-trfn/california-city-bans-predictive-policing-in-u-s-first-idUSKBN23V2XC; Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; Kashmir Hill, *How One State Managed to Actually Write Rules on Facial Recognition*, N.Y. TIMES (Mar. 5, 2021), https://www.nytimes.com/2021/02/27/technology/Massachusetts-facial-recognition-rules.html.

177. *See* Devich-Cyril, *supra* note 17.

178. *See* Chinyere Tutashinda & Malkia Cyril, *An End to the Mass Surveillance of Black Communities, and the End to the Use of Technologies That Criminalize and Target Our Communities (Including IMSI Catchers, Drones, Body Cameras, and Predictive Policing Software)*., MOVEMENT FOR BLACK LIVES, https://m4bl.org/wp-content/uploads/2020/05/End-Mass-Surveillance-Policy-Brief.pdf [https://perma.cc/9D62-BU2W].

179. *See* Moravec, *supra* note 129.

180. *See, e.g.*, Evan Selinger, *Q&A: The Battle over Face Surveillance Is About to Heat Up*, BOS. GLOBE (Apr. 28, 2021, 11:59 AM), https://www.bostonglobe.com/2021/04/28/opinion/qa-battle-over-

Civil Liberties Union (ACLU) of Northern California—with local assistance—succeeded in building a national coalition to ban facial recognition, resulting in local bans in significant cities such as San Francisco, Oakland, and Berkeley.[181] Across the country in Massachusetts, the ACLU—again with local support—successfully organized in Boston against facial recognition.[182] These complete bans were not only successful abolitionist policy wins for facial recognition, but they are some of the clearest legislative wins on any surveillance technology anywhere.[183] In addition, other surveillance oversight ordinances and entities came into existence with growing public support.[184]

2. Corporate Self-Restraint

Beyond political mobilization and legislative bans, a second result has been to pressure technology companies themselves. In 2020, Microsoft, IBM, and Amazon halted the sale of facial recognition services to law enforcement.[185] While these companies have been undercut by start-up ventures like ClearviewAI, which ignored calls to limit use, the symbolism of Big Tech deferring investment in law enforcement was significant, even if police departments

face-surveillance-is-about-heat-up/. Other advocacy leaders such as Alvaro Bedoya, Joy Buolamwini, Albert Fox-Cahn, Clare Garvie, Evan Greer, and Tawana Petty, and organizations such as the Detroit Community Technology Project, Stop Surveillance Oversight Project, Fight for the Future, Algorithmic Justice League, and the Georgetown Law Center on Privacy & Technology Center have also successfully advocated for a ban on facial recognition technology that drew national attention. *See, e.g.*, *Civil-Rights Group Letter to President Biden Calling for Facial Recognition Ban*, WASH. POST (Feb. 17, 2021), https://www.washingtonpost.com/context/civil-rights-group-letter-to-president-biden-calling-for-facial-recognition-ban/ad27090b-7b93-4f44-9ca9-1793157666b6/?itid=lk_inline_manual_4; *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, ELEC. PRIV. INFO. CTR. (June 3, 2021), https://epic.org/wp-content/uploads/privacy/facerecognition/Civil-Rights-Statement-of-Concerns-LE-Use-of-FRT-2021.pdf [https://perma.cc/EE9Z-XQJF]; Steve Neavling, *Just Say No to Facial Recognition, Says Detroit Coalition of Civil Rights Groups*, DETROIT METRO TIMES (Aug. 1, 2019, 3:14 PM), https://www.metrotimes.com/news-hits/archives/2019/08/01/just-say-no-to-facial-recognition-says-detroit-coalition-of-civil-rights-groups [https://perma.cc/9UVH-7NHZ].

181. *See* Conger et al., *supra* note 176; Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, S.F. CHRON. (July 17, 2019, 8:33 AM), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php/; Levi Sumagaysay, *Berkeley Bans Facial Recognition: It's Fourth U.S. City to Prohibit Public Agencies' Use of the Technology*, MERCURY NEWS (Oct. 16, 2019, 4:23 PM), https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.

182. *See* Nik DeCosta-Klipa, *Boston City Council Unanimously Passes Ban on Facial Recognition Technology: Marty Walsh's Office Says They Will Review the Ordinance*, BOSTON.COM (June 24, 2020), https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban [https://perma.cc/RT46-TM44].

183. *See* Susan Crawford, *Facial Recognition Laws Are (Literally) All over the Map: From Portland to Plano, Local Governments Are Placing Different Limits on the Use of Biometric Data. That's a Good Thing*, WIRED (Dec. 16, 2019, 8:00 AM), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map.

184. *See* CHIVUKULA & TAKEMOTO, *supra* note 42, at 1 n.1 (providing an excellent overview of existing local surveillance ordinances).

185. Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020, 2:30 PM), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition.

retained other avenues for accessing these tools.[186] This move of corporate self-restraint was not based on altruism but on community pressure. Activists targeted corporate America because of repeated media stories about growing surveillance power.

3. Theoretical Development

A final outcome has been the articulation of theories to ban—not just regulate—surveillance technologies. This abolitionist philosophy has helped reset debates about how hard to push against any accommodation in possible police adoption.[187] Such theories emerge from many places, but three distinct voices from different parts of the advocacy and scholarly spectrum offer clear examples of the tech abolitionist theory.

One voice comes from technology and race scholars, such as Professor Ruha Benjamin who published a book titled *Race After Technology: Abolitionist Tools for the New Jim Code*.[188] Professor Benjamin argues that society has coded societal inequality into our surveillance technology without seeing the bias inherent in the design.[189] The New Jim Code (like the New Jim Crow)[190] allows a new form of racial discrimination based on software code that is "designed to stratify and sanctify social injustice as part of the architecture of everyday life."[191]

Professor Benjamin calls for an abolitionist mindset that rejects reform models that reify existing power structures or fail to excavate the underlying racial biases in society.[192] The abolitionist goal is to reshape the "moral imagination" and create a "socially conscious approach to tech development that would require prioritizing equity over efficiency, [and] social good over market imperatives."[193] Most technological solutionism is just another line of Jim Code, superficially

186. *See* Ina Fried, *Clearview Brings Privacy Concerns from Facial Recognition into Focus*, AXIOS (Feb. 10, 2020), https://perma.cc/6DFY-A3GT.

187. *Cf.* Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy,'* ATLANTIC (Jan. 17, 2013), https://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283 (explaining information obscurity, and discussing the concept in relation to Facebook's new search tool, Graph, and other similar technologies, such as license plate readers, GPS trackers, and facial recognition tools). Professors Evan Selinger and Woodrow Hartzog have argued that facial recognition should be banned for all governmental and commercial purposes. *See* Woodrow Hartzog & Evan Selinger, Opinion, *Why You Can No Longer Get Lost in the Crowd: Once, It Was Easy to Be Obscure. Technology Has Ended That.*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html (noting that "obscurity is crucial to democracy" and that "[f]acial recognition technology poses an immense danger to society").

188. *See generally* BENJAMIN, *supra* note 27.

189. *Id.* at 160 ("The power of the New Jim Code is that it allows racist habits and logics to enter through the backdoor of tech design, in which the humans who create the algorithms are hidden from view.").

190. *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS (rev. ed. 2012) (arguing that the U.S. criminal justice system is a contemporary system of racial control, even though it adheres to the principles of colorblindness).

191. BENJAMIN, *supra* note 27, at 17.

192. *See id.* at 168.

193. *Id.* at 183.

improving a fundamentally broken carceral system. The abolitionist goals are broader. The shift requires rethinking who designs policing technology.[194] It encourages coded equity audits that would check for racial discrimination in technology and a democratized, independent group centered in the community that would oversee the technology.[195] Professor Benjamin offers a way to reimagine technology, not as a tool of surveillance but as a narrative of emancipation.[196] In providing the tools for abolition, Professor Benjamin provides the intellectual framework for a different approach to policing technologies—one that is radically decentered and deeply skeptical.[197]

No less compelling but far less academic is the argument put forward by grassroots activists who work together as the Stop LAPD Spying Coalition.[198] This group spearheaded the protests against predictive policing in Los Angeles and forced the LAPD to conduct the audit that eventually revealed the LASER program's flaws and ended PredPol's contract.[199] Their work in dismantling police, surveillance, and the entire "[s]talker [s]tate"[200] rests on a clear rejection of police power and what they call the Algorithmic Ecology of intersecting institutional layers of social control.[201] One of the most vocal critics of surveillance in Los Angeles is Hamid Khan, a community organizer and founder of the Stop LAPD Spying Coalition.[202] Khan has explained his antisurveillance mission in unapologetic terms.[203] For example, he stated:

194. *See id*. at 178–79.

195. *See id*. at 186–90.

196. *See id*. at 193.

197. *See generally id*. Other scholar activists have also helped develop the intellectual framework for a surveillance abolition critique. *See, e.g*., Brendan McQuade, *Police Surveillance Is Criminalization and It Crushes People*, COUNTERPUNCH (Oct. 15, 2020), https://www.counterpunch.org/2020/10/15/police-surveillance-is-criminalization-and-it-crushes-people/ [https://perma.cc/XLM8-U6NG]; Shakeer Rahman & Brendan McQuade, *Police Bureaucracy and Abolition: Why Reforms Driven by Professionals Will Renew State Oppression*, COUNTERPUNCH (Sept. 17, 2020), https://www.counterpunch.org/2020/09/17/police-bureaucracy-and-abolition-why-reforms-driven-by-professionals-will-renew-state-oppression/ [https://perma.cc/ZHC7-GUL7].

198. *See About Us*, STOP LAPD SPYING COAL., https://stoplapdspying.org/about-slsc/ [https://perma.cc/9QYR-SAXN] (last visited Oct. 20, 2021).

199. *See* Letter from Hamid Khan, Campaign Coordinator, Stop LAPD Spying Coal., to Mark P. Smith, Inspector Gen., Off. of the Inspector Gen. (May 8, 2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Ltr-to-OIG-May-8-2018-min.pdf [https://perma.cc/KB2U-VNAY].

200. *Fuck the Police, Trust the People: Surveillance Bureaucracy Expands the Stalker State*, STOP LAPD SPYING COAL. (June 24, 2020), https://stoplapdspying.org/surveillance-bureaucracy-expands-the-stalker-state/ [https://perma.cc/FY64-B2SF] [hereinafter *Fuck the Police, Trust the People*].

201. *See* Stop LAPD Spying Coal. & Free Radicals, *The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms*, MEDIUM (Mar. 2, 2020), https://stoplapdspying.medium.com/the-algorithmic-ecology-an-abolitionist-tool-for-organizing-against-algorithms-14fcbd0e64d0 [https://perma.cc/HP8G-7N7Y].

202. *See* Moravec, *supra* note 129.

203. *See* Tate Ryan-Mosely & Jennifer Strong, *The Activist Dismantling Racist Police Algorithms*, MIT TECH. REV. (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002709/the-activist-dismantling-racist-police-algorithms/ (documenting Khan's responses to interview questions about police surveillance, the coalition's guiding principles, and issues with predictive policing).

> We are fiercely an abolitionist group, so our goal is to dismantle the system. We don't engage in reformist work. We also consider any policy development around transparency, accountability, and oversight a template for mission creep. Any time surveillance gets legitimized, then it is open to be expanded over time.
>
> . . . .
>
> The goal is always to be building power toward abolition of these programs, because you can't reform them. There is no such thing as kinder, gentler racism, and these programs have to be dismantled.[204]

As the Stop LAPD Spying activists explain, surveillance reform policies—even with good intentions—are actually a step away from racial progress:

> Police reform is inherently anti-Black because it improves the operation of an institution that has been white supremacist at every moment of its history. Surveillance is the tip of policing's knife, and it originates in slave patrols, indigenous extermination, lantern laws (forcing Black people to illuminate their bodies in public), infiltration of organized dissent, and enforcement of apartheid.
>
> Surveillance bureaucratization can whitewash that history, allowing the state to treat surveillance as a mostly fine endeavor that occasionally tips into excess. This lets police claim community "approval" for their oppression. It also gives elite institutions yet more input in state violence (the history of wealthy funders capturing civil rights advocacy is long). And it puts lawyers – the profession most complicit in rebuilding and legitimating the carceral state – in greater control of police. In short, it makes policing more powerful, more lawful, and more difficult to dismantle.[205]

The argument combines several important themes discussed earlier: anti-Black history, co-opting control,[206] centering power with police and not with communities,[207] and a realistic view that nothing short of abolition will actually alter the existing carceral logic of coercive state power.[208] As a first-principles approach, abolition offers an intellectually consistent response. Banning all police and all police surveillance is the only escape from the technology trap.

---

204. *Id.*

205. *Fuck the Police, Trust the People*, *supra* note 200.

206. *See id.* ("Surveillance bureaucracy trusts police to self-audit and self-govern, when we know that police can never be trusted and that laws facilitating the use of police technology will be used to build new oppression.").

207. *See id.* ("Surveillance bureaucracy trusts that the concerns of those most harmed by surveillance will be well understood and represented by police and politicians, when all that these people consistently do is excuse or expand state violence.").

208. *See id.* ("Surveillance bureaucracy pretends policing can be reduced with new rules and criteria, when we know that this just leads police to invest more resources and personnel into monitoring and avoiding 'compliance.'").

The final voice comes from legal scholars who are building abolitionist theory around the protests of community groups. The argument to abolish the police finds roots in early movements to abolish prisons and the larger carceral solutions to poverty.[209] It looks to build alternative methods of social improvement that do not involve methods of social control like policing or incarceration.[210] The modern movement looks to defund, decenter, and end the role of police and police surveillance in poor communities. Professor Amna Akbar writes, "The movement is focused on shifting power into Black and other marginalized communities; shrinking the space of governance now reserved for policing, surveillance, and mass incarceration; and fundamentally transforming the relationship among state, market, and society."[211] Abolition includes the banning of surveillance technologies because those tools empower police, disempower individuals, and solidify the unequal distribution of coercive force.[212] The movement looks not to reform, because that would leave the status quo unchanged, but to a revolutionary shift in who controls the levers of coercive power.[213]

The logic of the trap lens involves a structural understanding of power. Because centuries of disenfranchisement, disinvestment, and discrimination through legal means have created the perceived need to police the resulting economic, social, housing, mental health, and educational gaps in society, the solution cannot be rooted in police. Fixing policing without simultaneously remedying the structural gaps in society will not alter the power dynamics.[214] Instead, the argument is that money and attention need to be diverted to address

---

209. *See* Roberts, *supra* note 161, at 19 ("Although prison abolitionists work to end prisons, their ultimate aspiration is to end carceral society — a society that is governed by a logic of incarceration."); *see also* ANGELA Y. DAVIS, ABOLITION DEMOCRACY, BEYOND EMPIRE, PRISONS, AND TORTURE 95–96 (2005); ANGELA Y. DAVIS, ARE PRISONS OBSOLETE? 28–36 (2003) (discussing Black and labor history in America).

210. *See* Akbar, *supra* note 169, at 412 ("Contemporary racial justice movements are not simply arguing the state has created a fundamentally unequal criminal legal system. They are identifying policing, jail, and prison as the primary mode of governing Black, poor, and other communities of color in the United States, and pointing to law as the scaffolding.").

211. *Id.* at 408 (footnote omitted); *see also* Allegra M. McLeod, *Envisioning Abolition Democracy*, 132 HARV. L. REV. 1613, 1615 (2019) ("Justice in abolitionist terms involves at once exposing the violence, hypocrisy, and dissembling entrenched in existing legal practices, while attempting to achieve peace, make amends, and distribute resources more equitably. Justice for abolitionists is an integrated endeavor to prevent harm, intervene in harm, obtain reparations, and transform the conditions in which we live.").

212. CHARLENE A. CARRUTHERS, UNAPOLOGETIC: A BLACK, QUEER, AND FEMINIST MANDATE FOR RADICAL MOVEMENTS, at x (2018) (defining abolition as "a long-term political vision with the goal of eliminating imprisonment, policing, and surveillance and creating lasting alternatives to punishment and imprisonment").

213. *Reformist Reforms vs. Abolitionist Steps in Policing*, CRITICAL RESISTANCE, https://static1.squarespace.com/static/59ead8f9692ebee25b72f17f/t/5b65cd58758d46d34254f22c/1533398363539/CR_NoCops_reform_vs_abolition_CRside.pdf [https://perma.cc/62P7-HCGE] (last visited Oct. 20, 2021) (stating that pushing for community oversight boards "further entrenches policing as a legitimate, reformable system, with a 'community' mandate. Some boards, tasked with overseeing them, become structurally invested in their existence").

214. *See* VITALE, *supra* note 24, at 30 ("Policing will never be a just or effective tool for community empowerment, much less racial justice.").

the structural lack of investment and political power in those same communities.[215] If done correctly, law enforcement will not be needed to police the gaps because the gaps will be filled by the community improving itself. In addition, the control over that community power will remain within the community.[216] The way to force such structural change is to end existing policing power, including enhanced police surveillance. Anything less is a trap that will be used against the powerless.

C. WHERE THE TRAP TEST FALTERS

The trap approach pushes absolute bans because bans are clear and unambiguous. And if you start from the first principle that policing is the problem (and thus technology that enhances police power must also be a problem), then there is little space for anything less than a ban. An uncompromising abolitionist would end the debate here: banning police technology and policing as we know it. The problem is that such a complete ban on policing is not politically feasible in the near term. Without addressing the social and economic gaps that generate criminal activity and without developing alternatives to police, abolishing all law enforcement will not happen overnight. Abolitionist theory presumes the creation of alternative forms of community safety to replace the need for police—alternatives that do not currently exist at scale.

Thus, if you concede some role for police, and decouple policing from police surveillance technologies, the question of whether police should be able to take advantage of advanced technology becomes more difficult. This is the challenge for those in the trap lens camp. Two related problems arise. The first is theoretical and the second political, and both turn on first-principles assumptions.

As theory, assuming police are going to be a part of society—even in a reimagined, decentered way—the question of their use of new technologies necessarily arises. Anything short of a complete ban requires line drawing in terms of what technologies are used, and who decides, how, why, where, and against whom the technologies are directed. Those questions likely find answers in existing democratic systems, which lead us down a more technocratic path; the technocratic lens will be discussed in the next Part.[217]

---

215. *See* Paul Butler, *The System Is Working the Way It Is Supposed to: The Limits of Criminal Justice Reform*, 104 GEO. L.J. 1419, 1475 (2016) ("I want to support a frame alignment around the term 'Third Reconstruction,' which some activists and scholars have used to refer to a coordinated effort to address institutional racism and inequality. The term is evolving to describe not only changes in public policy and legal doctrines, but also a broad-based social movement focused on racial justice."); I. Bennett Capers, *Afrofuturism, Critical Race Theory, and Policing in the Year 2044*, 94 N.Y.U. L. REV. 1, 59–60 (2019) (discussing the idea of "a Third Reconstruction" to address racial inequality (emphasis omitted)).

216. *See, e.g.*, *Community Control*, MOVEMENT FOR BLACK LIVES, https://m4bl.org/policy-platforms/community-control/ [https://perma.cc/LV6U-J3KW] (last visited Oct. 20, 2021) ("We demand a world where those most impacted in our communities control the laws, institutions, and policies that are meant to serve us . . . .").

217. *See infra* Part III.

Beyond a process argument, how do you determine the substantive limits of the technology? We know technologies exist that police believe can help them, so ban adherents need to make a normative claim of why government should blind officers to additional data that might be available and helpful. If police officers are recording data about crime reports, one needs to make an argument about why police administrators should not study that data for insights about future crime patterns. Why is predicting criminal risk from the data you already collect a problem? There are good arguments to be made on both sides, but once you concede the need for some response to crime, prohibiting the police from gaining access to available information needs an answer that will look less abolitionist and more regulatory.[218]

One answer might be to develop technology that avoids police and recenters community interventions for public safety. This seems to be the direction Professor Benjamin suggests in *Race After Technology*.[219] But even Professor Benjamin's call to rethink who designs the technology and add coded equity audits presumes some use of surveillance technology. Even with a democratized, independent group centered in the community that is conscious of building tools for emancipation and not incarceration, the end result is still building surveillance technology to monitor some subset of the population. And that type of technology is going to need someone to decide rules and policies, which forces line drawing that is again more regulatory than abolitionist.

More fundamentally, you need to make an argument about why policing does not deserve to evolve in a digital world. Almost every other professional enterprise has benefited from technological innovation, including data collection and analytics. It would be odd if police were unable to advance in similar digital ways (with smart cars, smart phones, digital video, data management systems, and predictive analytics). This argument is even odder when the pretechnological status quo was bad enough that it has led to for calls for police abolition.[220] Eliminating data-driven analysis just sends police back to the bad old days. While abolitionists have an answer to this puzzle (eliminate police), for those who concede police are necessary in some roles, there needs to be an answer to why this pretechnological solution is better than a data-driven version.

Demands for clear answers are not justifications for surveillance technologies per se. Police should have the burden of explaining why an innovation or data-driven insight is necessary and not harmful. Many innovations are likely misguided or involve too great a risk to privacy or civil liberties. But if some might add value, then the hard question becomes what renders certain upgrades more permissible than others. The point is that once you concede some role for police

218. There are also important differences between private data collection and government data collection, as well as important procedural hurdles that need to be raised, but those are process questions and not prohibition questions. Prohibiting the surveillance technology is the goal of many trap lens advocates. *See supra* Section II.B.

219. *See generally* BENJAMIN, *supra* note 27.

220. *See supra* notes 161–63 and accompanying text.

—even limited to investigating violent crime[221]—you need to engage in hard line-drawing questions about which technologies should be available to assist police and then come up with rules and policies for their use.[222]

The second problem is political. Sometimes the calls for technological bans are politically expedient but miss their mark. As an example, the campaign to ban place-based predictive policing and to end PredPol's contract with the LAPD offers an instructive tale about what success really means. As discussed earlier, PredPol in Los Angeles is a place-based predictive policing system that uses past crime data to "predict" where police should patrol to deter future crime.[223] In Los Angeles, the system focused on three crimes—burglary, car theft, and theft from automobile.[224] The inputs for the algorithm were rudimentary: calls for service from past crimes (such as "my home was burglarized" or "my car was stolen"), time, location, and type of crime.[225] Police officers were given paper printouts or computer maps of 500-by-500-foot areas of predicted crime and told to patrol.[226] Their task was to monitor those areas when not responding to ordinary calls for service. The hope was to be in the right place at the right time to deter crime.[227]

There are numerous criticisms of the PredPol model. I have previously written about constitutional, data, and efficacy concerns.[228] I have also questioned the gaps left behind at a structural level by focusing on certain crimes (property) as opposed to others (violent or interfamily offenses) and the opportunity cost of investing in data-driven policing at the expense of other social services.[229] Those problems and more have surfaced over the years. In fact, the LAPD Inspector General audit on PredPol revealed many flaws in application,[230] including data

221. The term "violent crime" has its own contested history. *See generally* DAVID ALAN SKLANSKY, A PATTERN OF VIOLENCE: HOW THE LAW CLASSIFIES CRIMES AND WHAT IT MEANS FOR JUSTICE (2021) (discussing the debate and choices around defining violent crimes).

222. The choice of what we consider crime is a contested definition that cannot be disentangled from racial and economic discrimination and practices. *See* Alec Karakatsanis, *Why "Crime" Isn't the Question and Police Aren't the Answer*, CURRENT AFFS. (Aug. 10, 2020), https://www.currentaffairs.org/2020/08/why-crime-isnt-the-question-and-police-arent-the-answer [https://perma.cc/BM2Q-BZHD] ("The concept of 'crime' is constructed by people who have power. Throughout history, powerful people have defined 'crime' in ways that benefit wealthy people and white people. For example, cocaine, marijuana, and opium were made illegal to target specific racial minorities. And even within categories of acts that are classified as 'crimes,' powerful people decide where to look for those acts, when to look for them, and which ones to ignore and which to document.").

223. *See supra* notes 85, 88–92 and accompanying text.

224. Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 267 (2012) (discussing the PredPol pilot).

225. *See id*. at 266–67.

226. *Id*. at 267.

227. *See id*. at 266–67.

228. *See generally* FERGUSON, *supra* note 6; Ferguson, *supra* note 8; Ferguson, *supra* note 111; Ferguson, *supra* note 224.

229. *See* FERGUSON, *supra* note 6, at 175 (discussing why it is easier to invest in policing than underlying social services).

230. OFF. OF THE INSPECTOR GEN., *supra* note 95, at 25–30.

collection,[231] officers' reluctance to obey an algorithm,[232] and most significantly, the complete inability to show if PredPol reduced crime by any meaningful measure.[233]

But those problems were not the justification that activists used to push a ban. Instead, the push to ban PredPol centered on claims of racism and a desire to limit any form of algorithm-enhanced policing.[234] This was a push for abolition because the trap lens allows no quarter for police, let alone technologically enhanced policing.[235] Examining the technology in the face of the evidence reveals that the attacks on PredPol were somewhat misdirected (even if successful). It also reveals the complexities of defaulting to an abolitionist trap lens.

The campaign to ban PredPol started with the claim that predictive policing was racially discriminatory.[236] It did so by focusing on two arguments, one quite defensible and one less so. The defensible claim is that all policing is racially discriminatory and so predictive policing is discriminatory.[237] The second is that because arrests are discriminatory and substantially dependent on patrol patterns and because drug arrests are discriminatory against Black and Latino people, PredPol uses a racist algorithm.[238] Unpacking these two arguments shows how the trap lens can blur policy choices.

As discussed earlier, policing has been structurally racist and discriminatory since the beginning.[239] Predictive policing, because it involves policing, will replicate this reality. This is absolutely true and is the basis of Professor Benjamin's indictment of the New Jim Code,[240] but it is also an argument against policing (not just predictive policing). Ending predictive policing does not alter the underlying problem of police power. Ending PredPol's contract with the LAPD did not reduce police patrols. It did not alter any racial bias or efforts at social control inherent in traditional policing. It just removed one data-driven tool, without

231. *See id.* at 27–29 (noting several collection issues such as "under- and over-reporting" by officers, "automated" data collection issues near or at LAPD facilities, and more).

232. *See id.* at 28–29 (detailing total visits and duration of visits at PredPol identified locations by LAPD vehicles).

233. *See id.* at 29–30 ("[T]he OIG's review of PredPol dosage revealed potential discrepancies with how dosage data is being collected that made it difficult to draw conclusions about the effectiveness of the system in reducing vehicle or other crime.").

234. *See, e.g.*, Lena Nguyen, Opinion, *Predictive Policing Algorithm Perpetuates Racial Profiling by LAPD*, DAILY BRUIN (May 2, 2019, 10:47 PM), https://dailybruin.com/2019/05/02/predictive-policing-algorithm-perpetuates-racial-profiling-by-lapd [https://perma.cc/N8YZ-6HY4].

235. *See supra* Section II.C.

236. *See Predictive Policing: Profit Driven Racist Policing*, STOP LAPD SPYING COAL. 2 (Dec. 7, 2016), https://stoplapdspying.org/wp-content/uploads/2016/12/Statement-of-Concern-on-Upturn-Predictive-Policing-Report-December-2016.pdf [https://perma.cc/59G8-65CM].

237. *See supra* Section II.A.

238. *See* Aaron Cantú, *Algorithms and Future Crimes: Welcome to the Racial Profiling of the Future*, SAN DIEGO FREE PRESS (Mar. 1, 2014), http://sandiegofreepress.org/2014/03/algorithms-and-future-crimes-welcome-to-the-racial-profiling-of-the-future/ [https://perma.cc/4UMU-ZMKX] (questioning whether predictive policing will perpetuate discriminatory arrests).

239. *See supra* Section II.A.

240. *See generally* BENJAMIN, *supra* note 27.

impacting the underlying power dynamics of who decides which policing technologies are deployed.

Second, the claims about discriminatory arrests and drug crimes as inputs would be absolutely correct if PredPol used either of those inputs in their system.[241] During the LAPD contract, PredPol never used arrests or drug crimes as inputs. The reason the racial bias argument gained traction was a study that hypothesized that if PredPol's algorithm—or any similar algorithm that "uses unadjusted police records to predict future crime[s]"—were used on drug arrests in Oakland, California, the resulting algorithm would be racially biased against minority communities.[242] The study presented a hypothetical model about a potential problem, offering a valuable warning to the use of predictive policing.[243] The study's authors were absolutely correct that it would be a racially discriminatory policing policy to use PredPol against drug crimes in Oakland. But this was not the reality of the actual technology being used in Los Angeles. This nuance was ignored by those who wanted to use the study to attack the technology as racist.[244] In fact, the PredPol inputs in Los Angeles avoided both identified problems by choosing calls for service for completed crimes and not arrests, and by choosing property crimes that have already occurred (not drug crimes).[245]

The point is not that PredPol avoids racial discrimination. Its own founders reported that PredPol essentially mirrors existing racial disparities of policing in Los Angeles (which has a history of racial discrimination), but that the fault for this difference lies in policing, not the algorithm.[246] From an abolitionist first-principles position (or trap lens), this is a distinction without a difference because,

241. From the original pilot study to the final audit, the PredPol system in Los Angeles focused on property crimes. *See* Ferguson, *supra* note 224.

242. Kristian Lum & William Isaac, *To Predict and Serve?*, SIGNIFICANCE MAG., Oct. 2016, at 14, 17–19; *see also* William S. Isaac, *Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice*, 15 OHIO ST. J. CRIM. L. 543, 547–53 (2018) (describing the study and responding to its critics).

243. *See* Lum & Isaac, *supra* note 242, at 19. I have both praised this study for warning about possible concerns and criticized it as being mischaracterized by many media outlets without correction. *See* Andrew Guthrie Ferguson, *The Truth About Predictive Policing and Race*, APPEAL (Dec. 7, 2017), https://theappeal.org/the-truth-about-predictive-policing-and-race-b87cf7c070b1 [https://perma.cc/EL8T-FVS5].

244. *See, e.g.*, Jack Smith IV, *Crime-Prediction Tool PredPol Amplifies Racially Biased Policing, Study Shows*, MIC (Oct. 9, 2016), https://mic.com/articles/156286/crime-prediction-tool-pred-pol-only-amplifies-racially-biased-policing-study-shows#.a7kBWFQyI [https://perma.cc/EM2F-LKZF].

245. Calls for service are not arrests. The former usually involve calls from a reporting victim for assistance after a past crime, so does not necessarily depend on police discretion. Arrests are generated from police making contact with an individual suspected of committing a crime and may involve discretion. Calls for assistance can occur without arrests and arrests can occur without calls for service. Burglaries, car thefts, and thefts from cars are types of crime that are regularly reported for insurance reasons and do not necessarily depend on police discretion. Some calls for service can reify racial bias, as one might imagine calls for "suspicious people" could be codewords for racial discrimination. But calls for car break-ins and burglaries fall outside of the challenged suspicion data and rest on more solid ground.

246. *See* P. Jeffrey Brantingham, Matthew Valasik & George O. Mohler, *Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Controlled Trial*, 5 STAT. & PUB. POL'Y 1, 5 (2018).

again, the goal is to abolish both policing and policing technology.[247] It is also a difference that does not justify use. If the technology does not improve racially disparate policing, that is reason enough not to use it. But the accusation of racial bias based on misdirected analysis (about drug arrest inputs in a different city) does show a rhetorical overreach for those who are not trying to ban both policing and predictive policing.[248]

Ironically, the final result from the victory of ending the PredPol contract was to have LAPD reinvest in yet other data-driven technologies, just without the catchy buzzwords.[249] A review of the LAPD 2019 - 2021 Strategic Plan shows an increase in data-driven metrics, including hotspot analysis and data-driven patrols.[250] The LAPD budget even increased, not decreased, after these trap-focused attacks.[251] While the plan does not claim to rely on predictive policing anymore, it does rely on analytics of past crime data to direct future patrols, which essentially doubles down on the same data collection and predictive analysis. While trap advocates should take credit for winning a significant early battle, the war is decidedly not over.

Equally important, the power of who controls surveillance did not change in Los Angeles. Advocacy resulted in the unilateral shutdown of one type of predictive policing by one vendor, but it was the police department's decision. Unlike some of the technocratic fixes suggested in the next Part, there is little stopping police administrators from signing a new contract with the next new name in surveillance technology. There is no legislative accountability, little institutionalized oversight, and no formal community power structure in Los Angeles. The actual

247. And there is good sense to this argument. If all policing is racist, adding racist technology to racist policing is not progress. *See supra* notes 202–08 and accompanying text (discussing the work of activists making this argument).

248. Perhaps as an admission of the limits of the direct critique but also as an acknowledgement of the structural powers at play, some activists have shifted to a more systemic critique. For example, when analysis was done about the location of the hotspots near Skid Row, activists from the Stop LAPD Spying Coalition concluded that the hotspots were not self-reinforcing feedback loops, as they would have been if tracking drug arrests; instead, they were designed to encircle areas of less economic wealth, essentially trapping those living in Skid Row with police presence. Stop LAPD Spying Coal. & Free Radicals, *supra* note 201. The data shows how police can be used to control areas economically and racially by relying on data-driven strategies. This result reveals similar effects of race-based discrimination, but it is a different argument that has been the dominant argument to rally opposition against the technology. *See id.* ("Given the prevailing notion that algorithmic policing would create 'feedback loops,' our expectation was to find Skid Row . . . to be laden with PredPol hotspots. But the hotspots were instead clustered at the periphery of the community. Rather than visualizing the hyper-policing that we know occurs in Skid Row, the PredPol hot spot maps appears [sic] to be drawing a digital border to contain, control, and criminalize Skid Row.").

249. *See* L.A. POLICE DEP'T, THE LOS ANGELES POLICE DEPARTMENT STRATEGIC PLAN 2019 - 2021, at 21–24, https://perma.cc/3LHK-EX94.

250. *See id.*

251. *See* Libby Denkmann, *LA City's $11.2 Billion Budget Boosts LAPD Spending and Dedicates $1 Billion for Homelessness*, LAIST (June 2, 2021, 4:05 PM), https://laist.com/news/politics/mayor-garcetti-signs-11-2-billion-city-budget-with-more-lapd-spending-1-billion-for-homelessness [https://perma.cc/7EH5-EYK7].

power to adopt or reject surveillance still rests exclusively in the control of police.

The coda to the Los Angeles fight was that the successful movement to attack PredPol as a manifestation of misguided predictive policing caused PredPol to change its name and modify its guiding philosophy. PredPol became Geolitica, and its focus (at least from marketing materials) turned to police technology that improves transparency, accountability, and effectiveness.[252] This branding move toward a more open, public-safety orientation is exactly the push the technocratic lens seeks to develop. As will be discussed in the next Part, this shift also fails to address the structural power dynamics at play in policing.[253]

D. CONCLUSION ON THE TRAP LENS

Trap lens arguments and the larger call to defund policing technology have reshaped the national debate. Although sweeping and ambitious, the call to completely dismantle surveillance systems has had real organizing appeal. The argument is intellectually consistent and—if one begins with the assumption that certain police departments will always protect property and privilege and thus be in the business of disciplining those who threaten those interests—accurate. In addition, in large urban police departments such as those in Los Angeles, Chicago, and New York City—which have never avoided scandal, corruption, and abuse—the argument that anything can avoid policing excesses rings hollow. Policing is the problem and surveillance-empowered policing is just a bigger problem.

The open question is whether the movement to abolish surveillance can work at scale. Early results show modest budget cuts and improved awareness around policing in general but fewer revolutionary changes.[254] In addition, political backlash has tempered transformative cultural change around policing. But momentum for big data policing technologies has noticeably slowed, and the warnings of the trap ahead have been heard loud and clear. Defunding police surveillance has become a more achievable proxy battle in the fight over police power and one that seems possible to win.[255]

III. THE TECHNOCRATIC LENS

On the spectrum between complete trust and abject distrust of policing surveillance, a third approach has emerged as a way to regulate the use of police

252. *See Trusted Services for Safer Communities: We Run Operations for Public Safety Teams to Be More Transparent, Accountable, and Effective*, GEOLITICA, https://geolitica.com/ [https://perma.cc/YQK3-NYPR] (last visited Oct. 22, 2021).

253. *See infra* Part III.

254. *See* Fola Akinnibi, Sarah Holder & Christopher Cannon, *Cities Say They Want to Defund the Police. Their Budgets Say Otherwise*, BLOOMBERG: CITYLAB (Jan. 12, 2021), https://www.bloomberg.com/graphics/2021-city-budget-police-funding/.

255. *See, e.g.*, DEFUND SURVEILLANCE, https://www.defundsurveillance.org/ [https://perma.cc/QF98-CA6C] (last visited Oct. 22, 2021) (detailing the Defund Surveillance campaign's demands to defund the police and surveillance).

technologies. Born out of a sense of reformist pragmatism, this technocratic approach emphasizes democratic accountability, external transparency, and internal front-end evaluations, policies, and limitations to cabin the use of new policing technologies. The idea is to avoid the obvious mistakes of early iterations of surveillance technologies, conduct front-end privacy and civil rights audits before launching the technology, then rigorously audit the practice on the back end. Some technologies might be banned, some allowed, but all would be rigorously evaluated for racial biases, privacy harms, and constitutional infringements. The hope is that the well-founded concerns about bias, opacity, and privacy could be minimized through rules and enforceable laws.

A. WHY REGULATE?

The urge to regulate has arisen from two overlapping ideas. First, as a matter of democratic theory, the idea that policing technology should be democratically accountable makes good sense in a democracy.[256] Second is the belief that the unforced errors of the first generation of surveillance technologies did not have to occur (even though they did).[257] The argument was made that much of the bias and discriminatory application could have been minimized (if not averted) with study, reflection, and planning that was conscious of the structural biases in society.[258] While a blanket trust approach had failed, a ban would not be necessary if certain reform measures could be adopted.

The hope was that a practical, technocratic approach to regulation and reform could offer concrete progress to those who wished to move past the binary stalemate between the trust and trap advocates. A technocratic approach offers insights from legal and technology experts to create a third way, neither trusting the technologies nor banning them but instead regulating them with due concern for privacy, liberty, civil rights, and the structural racial and power inequalities in which policing technologies operate.

1. Democratic Accountability

The technocratic approach begins with the belief that police have a role in ensuring public safety, but that this role must be democratically accountable.[259]

256. *See infra* Section III.A.1.

257. Error may, in fact, be a too charitable term, as the failure to see the harms caused by new technologies goes beyond good-faith inadvertence and into structural blindness and avoidance. The failure to foresee bias and future harms is a choice for which the technology creators should be held accountable.

258. A good example of this technocratic approach to the problems of government surveillance can be seen in the Federation of American Scientists' report on the future of digital surveillance. The report interviewed numerous stakeholders to examine how issues of bias, discrimination, and privacy harms could be minimized with better regulation and planning. *See generally* ISHAN SHARMA, FED'N OF AM. SCIENTISTS, A MORE RESPONSIBLE DIGITAL SURVEILLANCE FUTURE: MULTI-STAKEHOLDER PERSPECTIVES AND COHESIVE STATE & LOCAL, FEDERAL, AND INTERNATIONAL ACTIONS (2021).

259. *See* David Alan Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1706 (2005); Jonathan M. Smith, *Closing the Gap Between What Is Lawful and What Is Right in Police Use of Force Jurisprudence by Making Police Departments More Democratic Institutions*, 21 MICH. J. RACE & L. 315, 340–41 (2016).

This police role need not be the same role that caused deep concern about policing in recent decades, but some role is to be played (distinguishing this from the abolitionist position).[260] Surveillance technologies that enhance democratically legitimate policing also have a role if approved by democratic processes and if held accountable through democratic mechanisms.

Much of the theoretical work for democratic policing comes from legal scholars who have studied the undemocratic structure of policing.[261] As Professors Barry Friedman and Maria Ponomarenko have recognized, unlike many other agencies, police operate under little democratic authorization.[262] This fact raises both legitimacy concerns[263] and practical concerns and suggests that new forms of democratically connected rulemaking and oversight should be adopted.[264] Whether this oversight sounds in administrative rulemaking,[265] local involvement,[266] or

260. *See generally* Barry Friedman, Brandon L. Garrett, Rachel Harmon, Christy E. Lopez, Tracey L. Meares, Maria Ponomarenko, Christopher Slobogin & Tom R. Tyler, *Changing the Law to Change Policing: First Steps*, YALE L. SCH., https://law.yale.edu/sites/default/files/area/center/justice/document/change_to_change_final.pdf [https://perma.cc/2A58-LEP2] (last visited Oct. 22, 2021) (offering "immediate, concrete steps federal, state, and local governments can take to address enduring problems in policing").

261. *See, e.g.*, *Statement of Principles on Democratic Policing*, POLICING PROJECT, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/59dfa277a803bb57bb93252e/1510756941918/Democratic+Policing+Principles+9_26_2017.pdf [https://perma.cc/6CC6-RWTC] (last visited Oct. 22, 2021).

262. *See* Friedman & Ponomarenko, *supra* note 28, at 1843 ("Policing agencies—for that is what they are, agencies of executive government—fail to play by the rules of administrative governance. Because the usual requisites of democratic authorization are lacking with policing, we can have little confidence that policing at present is efficacious, cost-effective, or consistent with the popular will."); *see also* Ponomarenko, *supra* note 28, at 50–56 (characterizing policing as both "a problem *of* democracy" and a problem caused by the absence of democratic oversight); Renan, *supra* note 28, at 1091–92 (arguing for an administrative law approach to Fourth Amendment enforcement, in part to promote "greater . . . democratic accountability"); Slobogin, *supra* note 28, at 95, 140 (arguing that police departments must "accept the fact that they function in a democracy" and thus "should have to abide by the same constraints that govern other agencies").

263. *See* Joshua Kleinfeld, *Three Principles of Democratic Criminal Justice*, 111 NW. U. L. REV. 1455, 1483 (2017) ("[T]he administration and enforcement of criminal law should be *by* and *of* the people—that is, solidaristic, public, embedded in local communities . . . primarily under lay rather than official control . . . .").

264. *See* Friedman & Ponomarenko, *supra* note 28, at 1832 ("Rather than attempting to regulate policing primarily post hoc through episodic exclusion motions or the occasional action for money damages, policing policies and practices should be governed through transparent democratic processes such as legislative authorization and public rulemaking."); *see also* Joshua Kleinfeld, *Manifesto of Democratic Criminal Justice*, 111 NW. U. L. REV. 1367, 1371, 1374–77 (2017) (discussing "democratizing criminal justice"); Tracey Meares, *Policing and Procedural Justice: Shaping Citizens' Identities to Increase Democratic Participation*, 111 NW. U. L. REV. 1525, 1534–35 (2017) (discussing improvements in procedural justice as they relate to the possibility of ensuring "that all will be able to participate").

265. *See* Ponomarenko, *supra* note 28; Slobogin, *supra* note 28.

266. *See* Sunita Patel, *Toward Democratic Police Reform: A Vision for "Community Engagement" Provisions in DOJ Consent Decrees*, 51 WAKE FOREST L. REV. 793, 801 (2016) ("The primary theories of deliberative democracy emphasize the right, opportunity, and capacity of anyone subject to a collectively made decision to participate in a meaningful way in deliberations regarding decisions that affect him or her."); Fidler, *supra* note 28.

community contestation,[267] the goal is to have people (through their representatives) authorize the use of police power. These community-focused but technocratically led mechanisms and events would be spaces for democratic debate about the wisdom of adopting police surveillance technologies.

2. Foreseeable Errors

Another motivating force for the creation of technocratic solutions to surveillance technologies is that the original design errors were foreseeable. Almost every policing technology in recent memory was adopted without privacy risk assessments, published policies, or background analyses of the potential civil rights harms. Most were pushed out by technology companies trying to sell product, with police—not citizens—as the primary customer.[268] Legal experts and the impacted communities were almost never consulted before implementation. The results are observable in the mistakes detailed in the first Part of this Article, and most could have been predicted.

For example, using inputs that replicate policing patterns, not reported crimes, and targeting locations that correlate with socioeconomically disadvantaged areas raise legitimate bias concerns.[269] Using facial recognition technologies that are primarily trained on datasets of white, male faces with the resulting identification failures across race and gender is plainly mistaken (morally and practically).[270] These systems did not have to be built or developed the way they were. The blindness of structural racism and the lack of interest to think about systemic biases contributed to a flawed design process.[271] The simple truth is that in the rush to invent and sell new technology, companies chose to ignore the social, racial, or legal contexts of how the technology would be used in a world rife with inequality.

---

267. *See* Jocelyn Simonson, Essay, *The Place of "The People" in Criminal Procedure*, 119 COLUM. L. REV. 249, 265–66 (2019) ("An agonistic stance toward public participation in criminal legal institutions would allow groups to participate in the processes of those institutions while still remaining opposed to the dominant priorities of the state actors in charge of them. . . . In order to do so productively, such paths of critique must include and even prioritize the voices of those marginalized populations who are most directly impacted by criminal procedural practices. For it is the people at the bottom of the 'penal pyramid'—defendants, victims, and their families, friends, and neighbors who come from under-resourced neighborhoods—who are least likely to have the political power necessary to voice critiques of the system." (footnote omitted)).

268. *See supra* note 21 and accompanying text.

269. *See supra* notes 243–44 and accompanying text.

270. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 11 (2018) ("The most improvement is needed on darker females specifically."); Joy Buolamwini, *When AI Fails on Oprah, Serena Williams, and Michelle Obama, It's Time to Face the Truth*, MEDIUM (July 4, 2018), https://medium.com/@Joy.Buolamwini/when-ai-fails-on-oprah-serena-williams-and-michelle-obama-its-time-to-face-truth-bf7c2c8a4119 [https://perma.cc/AQC8-PQES] ("Error rates were as high as 35% for darker-skinned women . . . .").

271. *See* Joy Buolamwini, Opinion, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html ("A.I. systems are shaped by the priorities and prejudices — conscious and unconscious — of the people who design them . . . .").

The technocratic approach assumes that starting with those oft-ignored concerns can minimize the harms of the technologies. Just as bad inputs in a data-driven system generate bad outputs, good policy design generates good practices too.

B. RESULTS OF A TECHNOCRATIC LENS

The results of the technocratic approach to policing surveillance can be seen in rules, policies, audits, and academic reports that have sought to regulate surveillance technologies. The goal is to identify potential risks from inputs, socioeconomic–racial contexts, privacy harms, or other biases that could be avoided by limiting use. The goals of transparency, accountability, and fair process are central to the technocrat's toolkit. This Section examines how these goals can be operationalized through legislation, oversight boards, audits, and academic research.

1. Legislative Responses

The most comprehensive and successful technocratic response to police surveillance technology has been the Community Control Over Police Surveillance (CCOPS) movement.[272] Led by the ACLU and supported by dozens of civil rights groups,[273] the goal is to require local legislative permission before any new surveillance technology is adopted.[274] More than twenty jurisdictions have adopted some form of democratic check on the implementation of new technologies.[275] These laws are strong technocratic approaches, requiring actual legislative grants of authority as opposed to mere internal guidance or best practices subject to internal accountability.[276]

As a model legislative response, a CCOPS bill imagines a formal local ordinance that requires preapproval for all new surveillance technologies.[277] In addition, the operating legislation would require surveillance impact reports, use policies, annual audits, public hearings and reports, whistleblower protections,

272. Information on CCOPS can be found on the ACLU's webpage. *See Community Control over Police Surveillance: (CCOPS)*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance [https://perma.cc/6XVJ-4WYC] (last visited Oct. 23, 2021).

273. *See* Dave Maass, *Join the Movement for Community Control over Police Surveillance*, ELEC. FRONTIER FOUND. (Sept. 21, 2016), https://www.eff.org/deeplinks/2016/09/join-movement-community-control-over-police-surveillance [https://perma.cc/23HQ-LK7P] (describing the diverse coalition of groups involved).

274. For full disclosure, I have been an advocate of this approach to regulation. *See* Andrew Guthrie Ferguson, Opinion, *It's Time for D.C. to Regulate Police Surveillance Technology*, WASH. POST (June 26, 2020, 7:00 AM), https://www.washingtonpost.com/opinions/local-opinions/its-time-for-dc-to-regulate-police-surveillance-technology/2020/06/25/9e94feb6-b57a-11ea-aca5-ebb63d27e1ff_story.html.

275. *See Community Control over Police Surveillance: (CCOPS)*, *supra* note 272.

276. *See* Fidler, *supra* note 28, at 555–57 (describing some of the successes of the administrative approach).

277. Versions of the CCOPS bills also require review of technologies that police currently use. ACLU, AN ACT TO PROMOTE TRANSPARENCY AND PROTECT CIVIL RIGHTS AND CIVIL LIBERTIES WITH RESPECT TO SURVEILLANCE TECHNOLOGY 4 (2021), https://www.aclu.org/other/community-control-over-police-surveillance-ccops-model-bill [https://perma.cc/8YVU-NX34].

and legal remedies for failures to follow the law.[278] The goal is to make sure that jurisdictions have deeply considered the privacy and civil liberty risks of the technology, designed policies to minimize those risks, established auditing processes to double check the planned use, and developed feedback mechanisms from the community for public approval. The power of the legislation rests with the local governing body (usually a city council), but much of the work to develop impact statements, policies, audits, and reviews requires expert knowledge. Although not spelled out in the legislation, to work as designed, a CCOPS law needs experts in surveillance technology and privacy law to conduct risk analyses and write reports on behalf of the polity.

Although several cities have adopted the CCOPS model,[279] Seattle provides an example of how a CCOPS-like system works in practice.[280] As will be discussed, the CCOPS model requires significant investment in technical, political, and community-based oversight mechanisms.

The Seattle Surveillance Ordinance arose in response to a series of scandals involving surveillance technology being used without public notice.[281] Before any new surveillance technology is adopted, the ordinance requires a "[s]urveillance [i]mpact [r]eport," which includes "an in-depth review of privacy implications, especially relating to equity and community impact."[282] The ordinance requires community meetings and a public comment period as part of the surveillance impact report.[283] In addition, the Seattle City Council must review all new surveillance technologies before approval.[284] Finally, the ordinance requires "detailed reports on surveillance technology use, community equity impact, and non-surveillance technology acquisitions."[285] The Seattle ordinance covers all government surveillance technologies, not just police technologies, with "[s]urveillance" being broadly defined[286] and publicly detailed in a "master list."[287]

278. *Id*. at 1–8.

279. *See* CHIVUKULA & TAKEMOTO, *supra* note 42, at 1 & n.1 (examining the structure and scope of sixteen local surveillance ordinances).

280. *See About Surveillance*, SEATTLE.GOV, https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance- [https://perma.cc/CGU2-VKJW] (last visited Oct. 23, 2021); *see also* Rubinstein, *supra* note 43, at 1986–91 (discussing the history and practice of the Seattle Surveillance Ordinance).

281. *See* Rubinstein, *supra* note 43, at 1987.

282. *About Surveillance*, *supra* note 280.

283. *Id*.

284. *Id*.

285. *Id*.

286. *See id*. ("Surveillance is defined as technologies that 'observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.'").

287. CITY OF SEATTLE, MASTER LIST OF SURVEILLANCE TECHNOLOGIES 2, 5–10 (2019), https://perma.cc/W62D-ALCT ("The list in this report represents the best effort of departments to identify existing technologies based on the definition and criteria outlined in the Surveillance Ordinance. Should additional technologies that were in use as of September 1, 2017 be discovered, this report will be amended and resubmitted.").

As might be imagined, the time and effort to create surveillance impact reports, policies, and audits and to provide the Seattle City Council with the information needed to make decisions is quite substantial. The City hired a full time Chief Privacy Officer who oversees an office of privacy experts and legal professionals to fulfill the mandate of the ordinance.[288] Because the list of surveillance technologies is long and the front-end and back-end accountability documentation requirements so vast,[289] the workload has led to significant delays.[290] Perhaps more significantly for the technocratic lens, the work has been centered on privacy specialists who control the analysis and debate.[291] Although the final vote for approval is democratic, the bulk of the accountability rules are technocratic in nature.[292]

The CCOPS bills, and related model bills such as the New York City Public Oversight of Surveillance Technology (NYC POST) Act,[293] are positive steps toward transparency and accountability. The NYC POST Act resulted in the production of use policies for dozens of previously secret technologies by the NYPD.[294] Although the NYC POST Act lacks real enforcement mechanisms and has been criticized as too weak,[295] it does require transparent choices to be made about privacy, equity, and police power.[296] This, in turn, allows for public notice and comment.[297] Compared to a simple trust lens, the requirement to justify use

288. Rosalind Brazel, *City of Seattle Hires Ginger Armbruster as Chief Privacy Officer*, TECH TALK (July 11, 2017), https://techtalk.seattle.gov/2017/07/11/city-of-seattle-hires-ginger-armbruster-as-chief-privacy-officer/ [https://perma.cc/S99P-GLVV]. The Chief Privacy Officer's staff is a clear example of a technocratic approach to surveillance oversight. The individuals hired into these roles are well versed in technology, law, and compliance work.

289. The Seattle Surveillance Ordinance requires policies, audits, engagement, and reporting for each technology. *See supra* notes 282–85 and accompanying text. The documentation requirements of existing technologies consume a significant amount of time and effort.

290. Melissa Hellmann, *Seattle's Oversight of Surveillance Technology Is Moving Forward Slowly*, SEATTLE TIMES (June 5, 2019, 5:11 PM), https://www.seattletimes.com/business/technology/seattles-oversight-of-surveillance-technology-is-moving-forward-slowly/.

291. *See id.*

292. *See id.*

293. N.Y.C., N.Y., ADMINISTRATIVE CODE tit. 14, ch. 1, § 14-188 (2021), https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-124303 [https://perma.cc/NT84-XGVF]; *The Public Oversight of Surveillance Technology (POST) Act: A Resource Page*, BRENNAN CTR. FOR JUST. (Mar. 5, 2021), https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page [https://perma.cc/R4J7-SAHL].

294. *See* Lucas Ropek, *NYPD Announces How It Plans to Spy on You This Year*, GIZMODO (Jan. 14, 2021, 8:55 PM), https://gizmodo.com/nypd-announces-how-it-plans-to-spy-on-you-this-year-1846062795 [https://perma.cc/3E8F-MPBB]; *see also Policies*, N.Y.C. POLICE DEP'T, https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page [https://perma.cc/ET2P-ZZGR] (last visited Oct. 24, 2021) ("The Public Oversight of Surveillance Technology (POST) Act requires the NYPD to publish impact and use policies for the surveillance technologies used by the Department.").

295. Rebecca Chowdhury, *Abolishing Police Surveillance in NYC: Will Transparency Help or Make it Harder?*, SHADOWPROOF (Aug. 12, 2021), https://shadowproof.com/2021/08/12/abolishing-police-surveillance-in-nyc-will-transparency-help-or-make-it-harder/ [https://perma.cc/6YAG-AE7A].

296. *See The Public Oversight of Surveillance Technology (POST) Act: A Resource Page*, *supra* note 293.

297. The success of this notice and comment effort has been mixed. Advocacy groups, such as the Brennan Center for Justice, have compiled letters that criticize the NYPD for its lackluster response to

to a democratically elected body, even if in a technocratic manner, is a result that seems to be a modest improvement over the status quo.

2. Community Oversight Response

A legislative response centers oversight within democratic systems with elected representatives. Other democratic models center inclusive community groups to play a similar role.[298] The result of local oversight boards has been a more community-focused approach to surveillance reform.

The City of Oakland, California, for example, has developed one of the more prominent independent community oversight bodies.[299] In response to concern that Oakland was developing a Domain Awareness Center system without community input, a group of community organizers led by Brian Hofer began advocating for public oversight of all new surveillance technologies.[300] After several years, the city approved a standing Privacy Advisory Commission.[301] This commission is a body required to study and give advice about police surveillance technologies before implementation by the city.[302]

More specifically, the commission is a formal body of community representatives who offer technical advice to the city about the privacy risks of new surveillance, prepare public annual reports on existing surveillance technology, and oversee public hearings on government use of surveillance technologies.[303] In the policing context, the commission has created use policies for automated license plate readers,[304] cell site simulators,[305] unmanned drones,[306] and infrared thermal

draft surveillance policies. *See Public Comments in Response to the NYPD's Initial Disclosures Under the Public Oversight of Surveillance Technology (POST) Act*, BRENNAN CTR. FOR JUST. (Mar. 5, 2021), https://www.brennancenter.org/our-work/research-reports/public-comments-response-nypds-initial-disclosures-under-public-oversight [https://perma.cc/4SD5-KJXE].

298. *See, e.g.*, Fidler, *supra* note 28, at 556–57 (discussing the Seattle ordinance's inclusion of review by "a community stakeholder committee" and "wider community engagement provisions").

299. *See generally Privacy Advisory Commission*, CITY OAKLAND, https://www.oaklandca.gov/boards-commissions/privacy-advisory-board#page-documents [https://perma.cc/R28N-9T75] (last visited Oct. 24, 2021) (describing the Committee's functions and providing resources).

300. *See* Kate Conger, *The Man Behind San Francisco's Facial Recognition Ban Is Working on More. Way More.*, N.Y. TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/technology/facial-recognition-san-francisco-ban.html.

301. *See Bylaws*, CITY OAKLAND, https://cao-94612.s3.amazonaws.com/documents/Bylaws-for-the-Privacy-Advisory-Commission.pdf [https://perma.cc/ZU2P-QLNN] (last visited Oct. 24, 2021).

302. Alan Greenblatt, *What Cities Can Learn from the Nation's Only Privacy Commission*, GOVERNING (Feb. 21, 2020), https://www.governing.com/next/what-cities-can-learn-from-the-nations-only-privacy-commission.html.

303. *See* Oakland, Cal., Ordinance 13349 (Dec. 17, 2015), https://cao-94612.s3.amazonaws.com/documents/Privacy-Advisory-Commission-final-Ordinance-13349-CMS.pdf [https://perma.cc/A4LH-XWAE].

304. *See* MICHAEL P. FORD, CITY OF OAKLAND, PROPOSED USE POLICY FOR VEHICLE-MOUNTED AUTOMATED LICENSE PLATE RECOGNITION (ALPR) FOR PARKING MANAGEMENT AND ENFORCEMENT (2019), https://cao-94612.s3.amazonaws.com/documents/ALPR-Use-Policy_FINAL-APPROVED-BY-PAC_190617_231324.pdf [https://perma.cc/H7YG-9XG7].

305. *See Departmental General Order I-11: Cellular Site Simulator Usage and Privacy*, OAKLAND POLICE DEP'T, https://cao-94612.s3.amazonaws.com/documents/DGO-I-11-Cellular-Site-Simulator-Draft-Use-Policy-1.pdf [https://perma.cc/GGW7-NX7M] (last visited Oct. 21, 2021).

imaging cameras.[307] It has successfully helped ban facial recognition technology.[308] It has also created draft impact statements about various technologies, including the Domain Awareness Center system.[309] Most notably, Oakland (under the pressure of the advisory commission) passed a city ordinance requiring public approval before adopting new surveillance technologies.[310] This ordinance is akin to the Seattle legislation requiring impact statements, assessments, and public notice before adopting any new surveillance technology. The power of a Community Oversight Board ostensibly rests with the community through its representatives.

3. Independent Audits

The most technocratic responses to surveillance technology come from experts who audit surveillance systems. Independent audits have played an important role in regulating and shutting down certain technologies. In Los Angeles, the Inspector General of the LAPD conducted the formal audit that revealed the failures of the LASER program and PredPol.[311] In Chicago, the RAND Corporation had a central role in evaluating predictive policing programs.[312]

Independent audits can take many forms, but examining the RAND audit of the Chicago Police Department provides a useful example of how independent auditors can be a positive form of technocratic review. The RAND report on Real-Time Crime Centers in Chicago runs over seventy pages; addresses the technical specifics of different technologies, the process of information flow, organizational structures, socioeconomic and racial impacts, efficacy; and offers

306. *See* OAKLAND DEP'T OF TRANSP., [PROPOSED] USE POLICY FOR UNMANNED AERIAL VEHICLES (UAV)/DRONES, https://cao-94612.s3.amazonaws.com/documents/Proposed-Use-Policy_UAV120318.pdf [https://perma.cc/PR5E-T6PP] (last visited Oct. 24, 2021).

307. *See* Oakland, Cal., Resolution 85807 (Sept. 24, 2015), https://cao-94612.s3.amazonaws.com/documents/85807-CMS-FLIR-10-6-15.pdf [https://perma.cc/XVA5-LQY8] (last visited Oct. 24, 2021).

308. *See* Sarah Ravani, *Oakland Committee Approves Ban on Facial Recognition Surveillance*, S.F. CHRON. (June 25, 2019, 10:10 PM), https://www.sfchronicle.com/crime/article/Oakland-committee-approves-ban-on-facial-14050026.php. The Oakland Privacy Commission's recommendation to ban facial recognition shows that a technocratic approach can lead to abolitionist outcomes. Some technologies are deemed too dangerous to regulate and require a ban.

309. *See* Oakland, Cal., Resolution 85638 (June 2, 2015), https://cao-94612.s3.amazonaws.com/documents/DAC-Ad-Hoc-Policy.pdf [https://perma.cc/R28N-9T75] (last visited Oct. 24, 2021). In 2013, the city initiated discussions with the Port of Oakland to build a surveillance system with video cameras and other technology. *See* Ali Winston, *Oakland Surveillance Center Raises Concerns*, SFGATE (July 17, 2013, 9:46 PM), https://www.sfgate.com/crime/article/Oakland-surveillance-center-raises-concerns-4671708.php [https://perma.cc/BU4W-B3TJ]. Backlash against the idea spurred the creation of the Oakland Privacy Commission. *See* Greenblatt, *supra* note 302.

310. Oakland, Cal., Ordinance Adding Chapter 9.64 to the Oakland Municipal Code Establishing Rules for the City's Acquisition and Use of Surveillance Equipment (Apr. 26, 2018), https://oaklandca.s3.us-west-1.amazonaws.com/oakca1/groups/cityadministrator/documents/standard/oak070617.pdf [https://perma.cc/XEC8-GG7S] ("PAC Review Required for New Surveillance Technology Before City Council Approval"); *see PAC Surveillance Technology Ordinance Approved by City Council*, CITY OAKLAND (Jan. 20, 2021, 7:59 PM), https://www.oaklandca.gov/resources/pac-surveillance-technoloy-ordinance-approved-by-city-council [https://perma.cc/KL7L-DBSX].

311. *See* OFF. OF THE INSPECTOR GEN., *supra* note 95, at 1–30.

312. *See generally* HOLLYWOOD ET AL., *supra* note 56.

a history of the technologies with detailed citations and sources.[313] The authors follow established social science frameworks for analysis and provide significant documentation, charts, graphs, and data-driven analysis.[314] Whatever one's ultimate assessment of the audit's conclusions, it is unquestionably the work of experts who spent significant time detailing facts and analyzing those facts through established methodologies.

Importantly, both the LAPD Inspector General's audit and the RAND report led to the shuttering of predictive policing in Los Angeles and the Heat List in Chicago.[315] While it is evident that public protest and community sentiment shaped the ultimate decision to shut down the programs, the formal justification in both cases was the respective audit. Both audits used the police departments' own statistics, practices, and lack of policies to show that the systems could not be reformed. Spelled out with data, clear arguments, and technocratic conclusions, the audits made it difficult for decisionmakers to ignore the expert critiques.

A third example demonstrates how technologies can be audited to limit obvious privacy, liberty, and civil rights concerns. ShotSpotter is a company that sells acoustic sensors to identify gunshots.[316] As a stand-alone product,[317] the gunshot detector sensors consist of microphones deployed around a city to report when, where, and how many gunshots are detected.[318] A centralized incident review center collects the reports of gunshots and reports them to local authorities.[319] The technology is defended because it only collects the sounds of gunfire and allows quicker deployment of police and medical assistance to the location of detected gunshots. The concern is that police microphones across a city could capture conversations, violate people's sense of privacy, and target communities of color. In addition, these gunshot reports encourage an increased police presence by officers primed to respond to potential gun violence.[320] This response can

313. *See generally id.*

314. *See generally id.*

315. The link is not causal, but the timing of both shutdowns directly followed the audits.

316. Marin Perez, *Shots Fired: ShotSpotter Gunfire Detection System Provides Leg Up on 911*, POLICE1 (Sep. 25, 2007), http://www.policeone.com/police-products/police-technology/articles/1357787-Shots-fired-ShotSpotter-gunfire-detection-system-provides-leg-up-on-911/ [https://perma.cc/T5UZ-9DKV].

317. ShotSpotter sells other surveillance technologies to police, including a platform of data-driven policing technologies for patrol management. *See ShotSpotter Connect*, SHOTSPOTTER, https://www.shotspotter.com/law-enforcement/patrol-management/ [https://perma.cc/D2LU-FDRG] (last visited Nov. 20, 2021).

318. *See Reduce Gun Crime with Proven Gunshot Detection Technology*, SHOTSPOTTER, https://www.shotspotter.com/law-enforcement/gunshot-detection/ [https://perma.cc/C2S9-2MZL] (last visited Oct. 24, 2021).

319. Veronique Greenwood, *New Surveillance Program Listens for Gunshots, Get Police There in Minutes*, DISCOVER (May 30, 2012, 5:09 PM), http://blogs.discovermagazine.com/80beats/2012/05/30/new-surveillance-program-listens-for-gunshots-get-police-there-in-minutes/.

320. *See* Don Babwin & Sara Burnett, *Groups Say Gunshot Detection Systems Unreliable, Seek Review*, AP (May 3, 2021), https://apnews.com/article/chicago-police-crime-shootings-be9e44796bd7e6e3c94108c5e3905ede [https://perma.cc/68KS-SJ7W].

lead to police overreacting to perceived threats.[321]

Recognizing the privacy concerns arising from a technology that deploys mini microphones around the city, ShotSpotter retained the New York University (NYU) Policing Project to conduct a privacy audit of the technology.[322] The NYU Policing Project is an independent entity affiliated with the NYU School of Law that works to improve public safety through front-end democratic accountability.[323] The NYU Policing Project is staffed by law professors, lawyers, law students, and technologists who offer expert (and technocratic) insights on a host of privacy and civil rights issues.

The NYU ShotSpotter Privacy Audit offers a good example of how a deep dive into the technology and the surrounding privacy risks can avoid the unforced errors of other surveillance technologies, but it also reveals real limitations. First, the audit unearthed many design decisions that already minimized the inherent privacy risks of the audio recordings.[324] For example, sensor data is only stored for seventy-two hours and overwritten if no automated request is made.[325] Second, the sensor system primarily involves an algorithmic alert, with a human review of only a few seconds of audio files before and after the sound.[326] This process limits the amount of information heard by the analyst and purposely keeps the confirmatory audio file away from the police.[327] Finally, while the sensor technologies have the capacity to do more than record a particular type of sound, they are currently being utilized to only record audio files.[328]

The NYU Policing Project Privacy Audit built off of these technical limitations and suggested further privacy protective actions that ShotSpotter eventually

321. *See id*. The MacArthur Justice Center at Northwestern University Pritzker School of Law issued a report detailing how ShotSpotter encourages police violence in Black and Latino neighborhoods. The report suggests that the audio technology unnecessarily deploys tens of thousands of officers in response to alleged gunshots. *See* Press Release, MacArthur Justice Center, ShotSpotter Generated over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study (May 3, 2021), https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study [https://perma.cc/JQJ5-GHAY]; MacArthur Justice Center, *ShotSpotter Creates Thousands of Dead-End Police Deployments That Find No Evidence of Actual Gunfire*, END POLICE SURVEILLANCE, https://endpolicesurveillance.com [https://perma.cc/E82R-UZVE] (last visited Oct. 24, 2021).

322. *See* POLICING PROJECT, PRIVACY AUDIT & ASSESSMENT OF SHOTSPOTTER, INC.'S GUNSHOT DETECTION TECHNOLOGY (2019). The audit only addressed the privacy issues around the technology.

323. For several years, I have been an unpaid affiliate of the NYU Policing Project as a senior technology fellow. I was not involved in the drafting or analysis of the Policing Project's privacy audit of ShotSpotter.

324. *See* POLICING PROJECT, *supra* note 322, at 10–11 ("Once operational, these sensors are continuously 'listening' and a proprietary AI-enhanced algorithm is constantly analyzing incoming audio. The algorithm reviews the audio for loud 'impulsive' sounds—that is, loud sounds that start and end suddenly (similar to a gunshot). . . . Whenever ShotSpotter's algorithm detects an impulsive sound, the algorithm attempts to identify these sounds (e.g., 'gunfire,' 'helicopter,' 'construction'). Although all audio, including street noise, traffic, or human voice, are inputs to the algorithm, only gunshot-like sounds ('impulsive' sounds) actually trigger the sensor and the next stage of the process.").

325. *Id*. at 13.

326. *Id*. at 11–12.

327. *See id*. at 15.

328. *See id*. at 14.

adopted. The audit only focused on privacy risks and did not address efficacy, accuracy, or other racial justice or civil rights concerns. For example, the audit proposed a thirty-hour retention window for collected audio files, reduced from seventy-two hours.[329] Second, because of the privacy threat of omnipresent microphones, the audit proposed prohibiting disclosure of sensor locations to police.[330] While police would know where to go after a gunshot, they would be prohibited from knowing where the sensors exist in a city. Third, to respond to the concern of police obtaining audio footage of conversations around the gunshots, the company adopted the audit's suggestion to minimize audio collection to just the time of the gunshot and to oppose police subpoenas for potential audio content.[331] Among other recommendations, the audit also suggested avoiding placing sensors in sensitive areas such as churches, schools, health clinics, or areas that traditionally have served as public spaces for First Amendment-protected activities.[332] Each of these suggestions minimized the privacy risk of otherwise invasive surveillance devices.

The point is not to defend ShotSpotter but only to show how a technocratic understanding of a technology can minimize some harms at the front end.[333] If all surveillance companies took privacy concerns seriously and invited independent auditors into their design process, certain foreseeable design errors could be avoided. Planning on the front end and auditing the back end could avoid design mistakes and minimize harms. The choices of what to audit, who audits, and how to audit remains critical, however. For example, the NYU Policing Project Audit did not address the racial justice aspects of police responses in Black and Latino neighborhoods or the technology's potential to prime officers to be hypervigilant and thus too aggressive in their responses to potential gunshots.[334] Nor did the audit examine how audio files of suspected gunshots might be used or misused as evidence in criminal prosecutions.[335] Because the audit only focused on one aspect of the technology (privacy) and did not address other aspects of how the technology might impact civil liberties and civil rights, its value is limited. In addition, one can easily see how audits could be gamed to legitimize a process that provides no real accountability or improvement. Trap lens advocates will

329. *Id*. at 16.

330. *Id*. at 17.

331. *See id*. at 17–18.

332. *See id*. at 20.

333. There may be other harms beyond privacy. For example, the MacArthur Justice Center at the Northwestern Pritzker School of Law published a report that showed that ShotSpotter creates dangerous situations where police respond to potential gunfire with heighted concerns for weapons, adding to the likelihood of a deadly encounter. *See supra* note 321.

334. *See* Press Release, *supra* note 321.

335. *See* Garance Burke, Martha Mendoza, Juliet Linderman & Michael Tarm, *How AI-Powered Tech Landed Man in Jail with Scant Evidence*, AP (Aug. 19, 2021), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220 [https://perma.cc/22XK-DGHK]; Todd Feathers, *Police Are Telling ShotSpotter to Alter Evidence from Gunshot-Detecting AI*, VICE (July 26, 2021, 9:00 AM), https://www.vice.com/en/article/qj8xbq/police-are-telling-shotspotter-to-alter-evidence-from-gunshot-detecting-ai [https://perma.cc/94V4-BECS].

rightly be wary of an appeal to co-opt oversight through private contracting arrangements.

Audits are not a complete answer to the dangers of surveillance technology. Technical audits that identify privacy and civil liberties risks are only as good as their design, scope, and implementation. ShotSpotter as a company might follow best practices when it comes to privacy, but that does not mean that the police using ShotSpotter follow those same practices. For example, in one city, the technology was used to identify the sounds of illegal fireworks.[336] This use runs against both the audit and company guidelines, but when police buy the technologies, police also control their use.[337]

4. Academic Response

The final example of a technocratic response to policing surveillance comes from academia. In addition to conducting privacy audits for companies, the NYU Policing Project has developed model policies on technologies such as predictive policing, drones, social media surveillance, and automated license plate readers.[338] The goal of creating the policies was to help governments that are attempting to comply with local surveillance ordinances or wishing to establish best practices. Because drafting policies on technology is difficult in the best of circumstances, the model policies were meant to give police departments a head start on compliance.

In a similar fashion, the Harvard Law School's Criminal Policy Program and Stanford Law School's Criminal Justice Center collaborated to publish a Policy Toolkit for Emerging Police Technology.[339] The project was the result of two years of discussions and research between twenty-four law, technology, policing, and civil rights experts, as well as several teams of law students working on white papers on different technologies.[340] The audience for the toolkit is policymakers interested in thinking through the traps of new surveillance technology. The document provides a series of worksheets for police chiefs filled with questions about costs, governance, and community input that police departments should

336. *See* Caroline Haskins, *Police Departments Are Using Gunshot-Tracking Technology to Pinpoint Fireworks*, BUZZFEED NEWS (July 2, 2020, 7:28 PM), https://www.buzzfeednews.com/article/carolinehaskins1/police-surveillance-shotspotter-fireworks [https://perma.cc/ULP6-SZ92].

337. This fact is yet another data point that trap lens advocates would claim to demonstrate the lack of remedies for police misuse.

338. *See Resources*, POLICING PROJECT, https://www.policingproject.org/featured-resources [https://perma.cc/F3M9-E3U2] (last visited Oct. 24, 2021). I have directly worked, in an unpaid capacity, to create some of the policies proposed by the Policing Project.

339. *See generally* CRIM. JUST. POL'Y PROGRAM, HARV. L. SCH. & STAN. CRIM. JUST. CTR., STAN. L. SCH., EMERGING POLICE TECHNOLOGY: A POLICY TOOLKIT (2020) [hereinafter POLICY TOOLKIT], https://law.stanford.edu/wp-content/uploads/2020/01/Emerging-Police-Technology-A-Policy-Toolkit.pdf [https://perma.cc/J5LC-NTMT].

340. *See id.* at 3, 5. I was a paid Senior Visiting Fellow for the Harvard Law School Criminal Justice Policy Program and consulted extensively on the toolkit. For additional information on the Stanford–Harvard partnership on Policing and Technology, see Stanford Criminal Justice Center, *Policing and Technology*, STAN. L. SCH., https://law.stanford.edu/projects/policing-and-technology/ [https://perma.cc/H4WL-VZYV] (last visited Oct. 24, 2021).

consider.[341] The workflow requires front-end responses to minimize avoidable errors in design and to address community concerns.

Finally, law school programs such as the Berkeley Samuelson Law, Technology, & Public Policy Clinic, the University of Washington Tech Policy Lab, the Georgetown Law Center's Center on Privacy & Technology Program, and the NYU-affiliated AI NOW and Brennan Center have invested significant resources to respond to new policing surveillance technologies. Led by students and legal experts, these groups have written research reports, lobbied for legislative changes, and generated public awareness on the negative impacts of new surveillance technologies.

Each of these solutions shares the common belief that trust should not be the default for policing surveillance. Instead, some combination of external oversight, internal policy limits, and front-end accountability should be built into the structure of policing. The basic goal is to reform and regulate the growing power of police surveillance but not ban it outright. The push for reform centers on a combination of experts and community engagement, but the approach is primarily led by lawyers and technologists.

C. LIMITATIONS ON THE TECHNOCRATIC LENS

The technocratic lens suffers from real limitations on its effectiveness. Issues of enforcement, vision, and capacity limit any real hope of reforming powerful surveillance technologies in ways that do not continue to harm traditionally marginalized communities.

The first limitation involves structural power. The power of technology companies, police departments, and governments all require coequal checks on that power—checks that do not exist among technocrats or arise in academia. As a simple matter, remedies are lacking. Regulation requires accountability mechanisms that are not built into technocratic reforms. There is little penalty for failing to follow the policies. Even with strong legislative authority, real remedies are lacking to make police comply with the rules. What can a city council really do if the police fail to produce the required policies or audits? The currency of money and power corrupt attempts to create real forms of accountability. And, as has been discussed, this lack of accountability sits comfortably within the longstanding tradition of police departments resisting police reform.[342] An honest assessment of the first attempts at technocratic reform shows gains in transparency but not necessarily a limitation on police power.[343]

---

341. *See generally* POLICY TOOLKIT, *supra* note 339.

342. Many scholars have catalogued the failures of police reform. *See, e.g.*, Friedman, *Disaggregating*, *supra* note 61, at 928–29; Harmon, *supra* note 47, at 809–16; Alice Ristroph, *The Constitution of Police Violence*, 64 UCLA L. REV. 1182, 1188 (2017); Joanna C. Schwartz, *Who Can Police the Police?*, 2016 U. CHI. LEGAL F. 437, 438–39; Stoughton, *supra* note 46, at 613–14; Samuel Walker, *"Not Dead Yet": The National Police Crisis, a New Conversation About Policing, and the Prospects for Accountability-Related Police Reform*, 2018 U. ILL. L. REV. 1777, 1779–83.

343. *See* Fidler, *supra* note 28 (describing how administrative governance has fallen short).

The second limitation is also about power, but it is about how regulation reifies existing power structures.[344] As discussed with the trap lens, one reason why reform is a hollow victory for some advocates is that it normalizes the use of surveillance technology. The technocratic approach is basically a narrow reform response to the New Jim Code, not a movement against the idea of police surveillance. The technocratic lens offers moderate progress but leaves in place systemic inequality and increasing police power.[345] In fact, the regulatory structure may actually encourage the development of surveillance in ways that make it impossible to limit.[346] By creating a regulatory framework, it presumes that surveillance technology is needed and can be legitimatized with enough policies in place. Trap advocates have powerfully argued that technocratic reform is just a trust lens in different (and misleading) packaging.[347]

The third significant limitation is about perspective. The technocratic solution is almost always coming from a position of privilege. As can be seen in all of the examples discussed above, the policies, laws, or policy toolboxes were developed by lawyers and technologists (many from elite institutions) to be regulated primarily by the same groups.[348] These elite voices are protected by the privilege that policing traditionally guards and thus may not be centered in the communities impacted by police power. Some are funded directly or indirectly by the technology companies themselves, and most share a similar world view that police have some place in social order. The complicity between civil-society lawyers, academia, and police as reformers of the status quo, as opposed to revolutionaries against the status quo, means protection of the status quo.[349] This

344. *See* Bell, *supra* note 164, at 2147 ("The expansion of policing control has added to police departments' coffers over the past three decades, leading to the growth of many forces. Yet even police officers complain that the system expects them to play an outsized role in poor people's daily lives, performing functions that supplant work ideally done by the welfare state and social services." (footnote omitted)).

345. *See* Akbar, *supra* note 169, at 464–65 ("Two moves are essential to understand. First, the traditional police reforms that have been put forward—training, body cameras, better policies, more diverse police forces—do not address the underlying structural issues that manifest from and through white supremacy and capitalism. These reforms address superficial symptoms and perpetuate a system committed to anti-black racism. Second, the traditional reforms *may make the problem worse*. They advance a discursive universe that maintains confusion around the nature of the problem. They increase resources and legitimacy to the institutions that maintain inequality and systematic suffering." (footnotes omitted)); s*ee also* Allegra M. McLeod, *Envisioning Abolition Democracy*, 132 HARV. L. REV. 1613, 1618 (2019) (elucidating a vision for the future that focuses not on "alternative forms of prevention and redress of crime" but on "displac[ing] policing and imprisonment").

346. *See* Khan & White, *supra* note 18.

347. *See id.*

348. *See* Patel, *supra* note 266, at 803 ("'[D]eliberative democracy may be vulnerable to cooptation by elite members of the deliberative process, becoming a 'useful legitimating device[] for an already-decided policy.'" (second alteration in original) (quoting Carole Pateman, *Participatory Democracy Revisited*, 10 PERSPS. ON POL. 7, 9 (2012))).

349. *See generally* ALEC KARAKATSANIS, USUAL CRUELTY: THE COMPLICITY OF LAWYERS IN THE CRIMINAL INJUSTICE SYSTEM (2019) (calling out the complicity of lawyers in the criminal legal system); *see also* Karakatsanis, *supra* note 77, at 921–22 (arguing that elites "quell popular energy" for transformative change because they "are happy with the legal system and want it to keep functioning largely as it does").

cultural myopia creates blind spots in terms of who is harmed and who has a voice in the regulatory structures.[350]

Worse, the assumption of democratic legitimacy fails to acknowledge the gaps in democratic representation.[351] Many communities are, as Professor Monica Bell has described, legally estranged from police reform policies,[352] and many others are literally disenfranchised from the political process.[353] A reliance on democratic process when democracy is distorted by inequalities in cultural, social, and economic power is not, in fact, equal. While the technocratic process includes some voices of those impacted by the technologies and creates avenues for community empowerment, it is not centered in the community.

The final limitations involve capacity, consistency, and cost due to the scale of the policing systems in the United States. Policies are difficult to write.[354] Audits are expensive to conduct. Technologies change and then everything needs to be updated. Staying on top of dozens of different surveillance technologies spread out over almost 18,000 law enforcement agencies is an overwhelming task. Worse, only a few groups have the technical and legal capacities to analyze and audit the use of these technologies, and even these groups cannot keep up with demand. In addition, the localized nature of government means an equally fragmented appetite for oversight with relevant knowledge being unequally distributed. Adding to the complexity is the danger that companies will co-opt the

350. Even this Article, carefully dissecting analytical strains of arguments, is an example of privilege. The ability to discuss the abstract theories of surveillance governance without direct concerns about police power or personal consequence comes from a place of academic privilege.

351. *See* Bell, *supra* note 164, at 2067 ("[A]t both an interactional and structural level, current regimes can operate to effectively banish whole communities from the body politic."); *see also* Dorothy E. Roberts, *Democratizing Criminal Law as an Abolitionist Project*, 111 NW. U. L. REV. 1597, 1598–99 (2017) ("[T]he law enforcement bureaucracy is designed to operate in an anti-democratic manner. Therefore, democratizing criminal law requires an abolitionist . . . approach."); Jocelyn Simonson, *Democratizing Criminal Justice Through Contestation and Resistance*, 111 NW. U. L. REV. 1609, 1610–13 (2017) (positing that "America's criminal justice system is anti-democratic" because it is unresponsive to the needs of the people "most likely to come into contact with [it]," whose voices are systematically "muted").

352. Bell, *supra* note 164, at 2066–67 (describing a theory of "*legal estrangement* to capture both legal cynicism — the subjective 'cultural orientation' among groups 'in which the law and the agents of its enforcement, such as the police and courts, are viewed as illegitimate, unresponsive, and ill equipped to ensure public safety' — and the objective structural conditions (including officer behaviors and the substantive criminal law) that give birth to this subjective orientation" (footnotes omitted) (quoting David S. Kirk & Andrew V. Papachristos, *Cultural Mechanisms and the Persistence of Neighborhood Violence*, 116 AM. J. SOCIO. 1190, 1191 (2011))).

353. *See* Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 145 ("Structural inequity permeates American society to an extent that is impossible to summarize here, but some notable examples that are relevant to police technology include race-based residential segregation, a criminal legal system that perpetually disadvantages black people, political disenfranchisement of people who have been convicted of crimes, a culture that ties blackness to criminality, and a legal system that helps to insulate police behavior from scrutiny and accountability.").

354. As a result, for-profit groups have emerged to write policies for police. *See* Ingrid V. Eagly & Joanna C. Schwartz, *Lexipol: The Privatization of Police Policymaking*, 96 TEX. L. REV. 891, 892–99 (2018) (describing how private groups have been developing policies for police on a national level).

oversight through financial incentives or corporate support.[355] Issues around big technology companies funding reform projects raise red flags about objectivity and vision. Until communities can build public oversight capacity, there may not be enough resources to even attempt a technocratic response to surveillance technologies.

D. CONCLUSION ON THE TECHNOCRATIC LENS

The technocratic lens is definitely an improvement over the trust approach because it offers a measure of democratic accountability and oversight. But as stated above, the inherent gaps and limitations make reliance on a pure technocratic approach a bit naïve. Oversight should work, but the question is whether it will work in practice without power to check policing institutions themselves. Rules without remedies offer only paper promises without practical power. And, as trap lens advocates note, reform may hide the real harms in bureaucratic language.[356] Embracing reform may appear constructive but, in practical effect, may just enhance police power to protect property, privilege, and other powerful interests. As long as democracy remains co-opted by money, influence, and cultural power, many marginalized communities will be without a vote to limit police surveillance.

IV. THE TYRANT LENS

In contrast to the technocrat's focus on plans and policy, the tyrant lens focuses on power. Because surveillance technology offers government a new power to monitor and control citizens, the response must check that power. The question is how, and the answer is to assume the worst. Power will be abused, and constraints must work backward from that cynical starting point. The tyrant lens assumes that governmental power, including police power, must be checked (and checked again) because the government will misuse it against the less powerful.

As a first principle starting point, the tyrant test remains deeply skeptical of new forms of technological surveillance power, requiring equally powerful institutional checks that decenter government power into overlapping community institutions with enforceable individual rights. Technocratic policies, best practices, and oversight steps are necessary but not sufficient to address the threat that policing technology will be misused against those without power. At the same time, the tyrant lens is not abolitionist, conceding the utility of some policing technology under heavy restriction.

---

355. *See, e.g.*, Alex C. Engler, *Independent Auditors Are Struggling to Hold AI Companies Accountable*, FAST CO. (Jan. 26, 2021), https://www.fastcompany.com/90597594/ai-algorithm-auditing-hirevue.

356. *See* Karakatsanis, *supra* note 77, at 921 (arguing that "punishment bureaucrats create confusion" by "marketing little tweaks as huge changes," or "quelling popular energy for dramatically changing the punishment system").

Tyranny—and the fear of arbitrary power—rests at the center of our constitutional order.[357] As will be detailed, the tyrant test can claim a historical pedigree dating to the Founding of the country and the original spirit of the Fourth Amendment. In addition, the tyrant test finds support in the Fourteenth Amendment as a direct response to the arbitrary and oppressive Southern policing practices that enforced slavery, peonage, and the broader structural power of racial oppression.[358] Tyranny, be it British customs agents or Southern slave patrols, manifested as forms of arbitrary police-surveillance power that necessitated a constitutionally grounded, structural response.[359]

This Part attempts to reclaim the tyrant test as a better response to police surveillance technologies. The idea is to develop a first-principles framework to assess surveillance that builds off Fourth Amendment insights. The goal is not to suggest a new Fourth Amendment rule but to recognize that our old constitutional responses to other tyrannical threats have application anew. America has faced the threat of tyranny before and has responded using similar requirements, structures, and rights codified in our foundational law.[360] As metaphor and structural framework, the original Fourth Amendment inspires a tyrant test that only certain surveillance systems can pass.

A. WHY A FOURTH AMENDMENT FRAMEWORK?

New surveillance technologies present the question of how to face the potential threat of tyrannical power. The response to actual tyranny can take many forms: protest, revolution, civil war, coup, or other forms of social and political change. But the threat to potential tyranny—of democratically handing over the levers of coercive state power to potential misuse—is a once-removed concern. What do you do to at the front end to prevent the potential misuse of government police power at the back end?

Although the U.S. Constitution is only one possible answer to this problem, it is ours as Americans, and it offers some important insights about how to move forward in the face of potential surveillance tyranny.[361] This Section examines the lessons the Fourth Amendment offers against traditional forms of tyranny, surveillance, and racial discrimination in an effort to develop future protections for digital forms of mass surveillance. As originally understood, the Fourth Amendment was far less trusting of government power than modern law

357. *See infra* Section IV.A.1.

358. *See infra* Section IV.A.3.

359. *See infra* Sections IV.A.2–3.

360. *See* Moran, *supra* note 35, at 958 ("The United States has not always been deferential to police. To the contrary, distrust of law enforcement was a hallmark of the pre-Revolutionary War colonies, and that distrust heavily influenced the founders of this country.").

361. *See* TIMOTHY SNYDER, ON TYRANNY: TWENTY LESSONS FROM THE TWENTIETH CENTURY 10 (2017) ("[T]he Founding Fathers sought to avoid the evil that they, like the ancient philosophers, called *tyranny*. They had in mind the usurpation of power by a single individual or group, or the circumvention of law by rulers for their own benefit.").

allows.[362] It was neither technocratic nor abolitionist, but instead it offered a deeply skeptical compromise about power, the potential misuse of power, and the structural restraints on power.[363]

Many scholars have debated the history of the Fourth Amendment.[364] Many more have used Fourth Amendment history to craft new theories for a modern age.[365] And, a few scholars have rightly cautioned that any historical analysis based on an era without a professional police force, without exclusionary remedies, and without extensive criminal laws is a misleading place to begin an analysis.[366]

Conceding the complexities and inconsistencies of the historical record, two (almost) uncontested principles emerge from an examination of the original Fourth Amendment. First, the Fourth Amendment was a response to a threat of tyrannical governmental power.[367] Second, the Fourth Amendment was a response to authorized, but oppressive, government surveillance.[368] For our purposes—attempting to find first principles from which to approach new police surveillance technologies—this consensus suffices. The Founders feared tyranny and government surveillance into private spaces and crafted a system of enforceable rights and decentralized power centers to protect the people from government overreach.[369] The Founders viewed surveillance through a tyrant lens and so should we.

---

362. *See* Eric F. Citron, Note, *Right and Responsibility in Fourth Amendment Jurisprudence: The Problem with Pretext*, 116 YALE L.J. 1072, 1078 (2007) (describing the "power-skeptical" stance of the Fourth Amendment).

363. *See infra* Section IV.B.

364. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994); Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 983–84 (2011); Morgan Cloud, *Searching Through History; Searching for History*, 63 U. CHI. L. REV. 1707, 1720–43 (1996); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 576–78 (1999); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1185–93 (2016); Donald Dripps, *Akhil Amar on Criminal Procedure and Constitutional Law: "Here I Go Down That Wrong Road Again,"* 74 N.C. L. REV. 1559, 1561–63 (1996); Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 929 (1997); David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1805 (2000); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 846–57 (1994).

365. Any string cite of scholarship would not do justice to the scores of excellent articles on new technology and the Fourth Amendment. You know who you are and thank you.

366. *See, e.g.*, Richard M. Re, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885, 1921 (2014) ("Due to the lack of police, the Fourth Amendment received relatively little judicial attention for most of the nineteenth century."); Steiker, *supra* note 364, at 824 ("[A]t the time of the drafting and ratifying of the Fourth Amendment, nothing even remotely resembling modern law enforcement existed.").

367. *See, e.g.*, David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B. U. L. REV. 425, 452–53 (2016) ("Like many provisions of the Bill of Rights, the Fourth Amendment was motivated by the experiences of colonials and their British brethren with abuses of power.").

368. *See, e.g.*, Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

369. *See infra* Sections IV.A.1–2.

1. Tyranny

Tyranny is a strong charge. Evocative in argument and rhetorically powerful, it conveys a fear of despots and kings.[370] But such was the actual fear at the time of the Founding. Having lived through the reign of King George III, the Founding Generation did not want to empower a new federal government only to repeat the same abusive mistakes.[371] The Constitution was a hedge against tyranny.

This focus on tyranny, literal and theoretical, can be found in the words of the Founding Generation, which directly evoked fears of tyranny as a justification for the constitutional system.[372] These fears have been echoed in court cases spanning centuries on the justification behind the Fourth Amendment.[373] The feared tyranny took many forms: concerns about political repression, arbitrary investigations, economic confiscation, and a host of now familiar grievances that led to the

370. *See* Stephen F. Rohde, *Presidential Power vs. Free Press*, L.A. LAW., Oct. 2017, at 26, 26 ("The political thinkers who founded America designed a government to serve as a barrier against the tyranny they had experienced under King George III and the history of European despots they knew only too well.").

371. *See* AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 63–64 (2005) (describing the separation of powers as a means to protect against tyranny).

372. *See* Donohue, *supra* note 364, 1250 ("Otis denounced general warrants as a tyrannical exercise of power. 'I will to my dying day oppose,' he stated, 'with all the powers and faculties God has given me, all such instruments of slavery on the one hand, and villainy on the other, as this writ of assistance is.'" (quoting M.H. SMITH, THE WRITS OF ASSISTANCE CASE 552 (1978))); Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1371 (1983) ("Political historians have debated whether and by how much the writs of assistance contributed to the coming of the Revolution. . . . What *is* important is that the fourth amendment emerged from the colonists' experiences with general warrants and writs of assistance as tools of censorship and tyranny.").

373. *See, e.g.*, United States v. Hunt, 505 F.2d 931, 936 (5th Cir. 1974) ("The [Fourth] Amendment was enacted while the memory of British tyranny was fresh in the minds of the Founding Fathers."); Wrightson v. United States, 222 F.2d 556, 559 (D.C. Cir. 1955) ("The [Fourth] Amendment protects the people against the seizure of their persons as well as against the search of their houses. . . . Such searches and seizures are the embryo of tyranny, and [the Founders] well knew it. Once those safeguards are gone, the supremacy of force is complete, potentially even if not presently factually."); United States v. Zemlyansky, 945 F. Supp. 2d 438, 452 (S.D.N.Y. 2013) ("The Fourth Amendment requires that warrants state with particularity the items to be searched and seized. This requirement traces directly back to the Framers' experience of tyranny before this Nation's founding . . . ."); United States v. Browning, 634 F. Supp. 1101, 1102 (W.D. Tex. 1986) ("The Fourth Amendment of the United States Constitution was written to protect Americans from government tyranny."); United States v. Silverman, 166 F. Supp. 838, 840 (D.D.C. 1958) ("The history of the Fourth Amendment shows that it was based on the famous decision of Lord Camden, as well as the experience of the colonies in connection with writs of assistance and was intended to bar exploratory domiciliary searches that were obviously oppressive and savored of tyranny."), *aff'd*, 275 F.2d 173 (D.C. Cir. 1960), *and rev'd*, 365 U.S. 505 (1961); Underwood v. State, 78 S.E. 1103, 1106 (Ga. Ct. App. 1913) ("They are the sacred civil jewels which have come down to us from an English ancestry, forced from the unwilling hand of tyranny by the apostles of personal liberty and personal security. They are hallowed by the blood of a thousand struggles; and were stored away for safe-keeping in the casket of the Constitution. It is infidelity to forget them; it is sacrilege to disregard them; it is despotic to trample upon them. They are given as a sacred trust into the keeping of the courts, who should with sleepless vigilance guard these priceless gifts of a free government.").

U.S. Constitution and the Bill of Rights.[374] Tyranny was thus not just a motivating force but a framing fear of the constitutional order.[375]

A modern tyrant test draws from this historical background. The tyrant is not just a rhetorical trope but a real fear of lawful, but oppressive, government. Although the democratic process has distanced us from this proverbial tyrant (for the most part), the fear of government overreach remains. Designing legal structures to prevent tyrannical power via surveillance technology is consistent with—if not required by—the constitutional plan.

2. Surveillance Power

The colonial threat of tyranny was not abstract but concretely manifested in specific policing powers.[376] Customs agents and royal government ministers policed the colonies by authorizing broad searches and seizures of people, property, and goods.[377] The colonists lived in a quasi-surveillance state with British agents tasked to monitor, inspect, and control towns for economic and political reasons.[378] In preconstitutional revolutionary days, the potential use of general

374. The Fourth Amendment worked as a bulwark against tyranny in conjunction with other constitutional rights such as the right to a jury and the Fifth Amendment. *See, e.g.*, Allen v. Illinois, 478 U.S. 364, 383 (1986) (Stevens, J., dissenting) ("[T]he Fifth Amendment can serve as a constant reminder of the high standards set by the Founding Fathers, based on their experience with tyranny." (quoting ERWIN N. GRISWOLD, THE FIFTH AMENDMENT TODAY 81 (1955))); Pereira v. Farace, 413 F.3d 330, 337 (2d Cir. 2005) ("The right to trial by jury has long been an important protection in the civil law of this country. According to the Founding Fathers, the right served as 'an important bulwark against tyranny and corruption.'" (quoting Parklane Hosiery Co. v. Shore, 439 U.S. 322, 343 (1979) (Rehnquist, J., dissenting))).

375. *See* Charles E. Moylan, Jr. & John Sonsteng, *Constitutional Constraints on Proving "Whodunnit?,"* 16 WM. MITCHELL L. REV. 171, 182 (1990) ("Many of the leading figures from the independence movement such as Patrick Henry, Samuel Adams, Governor Clinton of New York and Governor Randolph of Virginia vehemently opposed the proposed constitution as 'a return to tyranny.'").

376. *See* Gray, *supra* note 367, at 453 ("Among English courts' primary reasons for outlawing general warrants was their effect on collective security. The courts reasoned that nobody could feel secure if forced to live under a regime where executive agents had the authority to engage in programs of broad and indiscriminate search, limited only by their own unfettered discretion." (footnote omitted)); James J. Tomkovicz, California v. Acevedo*: The Walls Close in on the Warrant Requirement*, 29 AM. CRIM. L. REV. 1103, 1134 (1992) ("The Framers objected to general warrants and writs of assistance because they resulted in arbitrary deprivations of privacy, property, and liberty. Those deprivations were arbitrary in part because officers were authorized to search and seize upon bare suspicion. They were also arbitrary and dangerous because agents of the executive were given 'unlimited discretion' to choose whom, where, and what to search and seize." (footnotes omitted)).

377. The protections ran to commercial establishments as well. *See* Donohue, *supra* note 364, at 1261 ("John Dickinson wrote *Letters from a Pennsylvania Farmer*, a series of essays decrying the Townshend Acts. 'By the late act,' he wrote, [']the officers of the customs [were] impowered to enter into any HOUSE, warehouse, shop, cellar, or other place, in the British colonies or plantations in America to search for or seize prohibited or unaccustomed goods, etc. on writs granted by the superior or supreme court of justice, having jurisdiction within such colony or plantation respectively.[']" (second alteration in original)).

378. As is well understood, the blanket authority granted to British agents to search and seize goods created frustration and resentment in the colonies. General warrants allowed almost indiscriminate searches, authorizing the holder of the warrant almost unlimited access to go into homes and businesses to search for contraband, seditious material, or untaxed goods. Writs of assistance were particular forms

warrants and the writs of assistance as enforcement authorities mobilized colonists to rebel.[379] After independence, the fear of federal search powers motivated states to pass search and seizure protections, which eventually inspired the Fourth Amendment.[380]

Responding to potential invasive surveillance powers thus was at the center of the original Fourth Amendment.[381] These government powers involved mechanisms of social control and policing. For example, general warrants were overbroad and essentially permanent, granting surveillance powers without geographic or temporal boundaries.[382] In addition, general warrants allowed for arbitrary monitoring and confiscation, placing discretion in the hands of individual agents of the state.[383] Third, the surveillance directly impacted specific interests, such as

---

of general warrants that authorized searches in Boston and other colonial cities in the mid-1700s. The anger that arose in response to these broad grants of unchecked power sparked the American Revolution. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 70 (2013) ("Before America's founding, British agents routinely abused general warrants, including writs of assistance, to subject our forefathers to the eighteenth-century equivalent of a surveillance state.").

379. *See* Gray, *supra* note 367 ("The Fourth Amendment's principal *bêtes noires* were general warrants, including writs of assistance.").

380. *See* Sklansky, *supra* note 364, at 1792 ("[D]uring the debates at the state level over ratification of the proposed Constitution, those concerned about the search-and-seizure powers of the federal government consistently called for an amendment restraining those powers 'within proper bounds,' or forbidding 'all unreasonable searches and seizures.'").

381. *See, e.g.*, Riley v. California, 573 U.S. 373, 403 (2014) ("Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself."); *see also* Donohue, *supra* note 364, at 1284 ("Concerns about general warrants, and about ensuring that specific warrants contained sufficient particularity, figured largely in the conversation, which centered on ensuring that the rights of the people would be secure against government overreach.").

382. *See, e.g.*, Stanford v. Texas, 379 U.S. 476, 481 (1965) ("Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws. They were denounced by James Otis as 'the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book,' because they placed 'the liberty of every man in the hands of every petty officer.'"); Wheeler v. State, 135 A.3d 282, 297 (Del. 2016) ("[I]nitial efforts at crafting a Federal Constitution met strong opposition due, in part, to the drafters' failure to impose limits on the government's power to search. These objections ultimately led to the inclusion of the Fourth Amendment in the Federal Bill of Rights." (footnote omitted)).

383. *See, e.g.*, Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."); Camara v. Mun. Ct., 387 U.S. 523, 528 (1967) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."); Draper v. United States, 358 U.S. 307, 319–20 (1959) (Douglas, J., dissenting) ("When the Constitution was up for adoption, objections were made that it contained no Bill of Rights. And Patrick Henry was one who complained in particular that it contained no provision against arbitrary searches and seizures: '. . . general warrants, by which an officer may search suspected places, without evidence of the commission of a fact, or seize any person without evidence of his crime, ought to be prohibited. As these are admitted, any man may be seized, any property may be taken, in the

the home, persons, papers, and effects.[384] Compared to modern law enforcement, early police had few investigative powers, but the fear of authorizing greater surveillance power remained real. The debates about how to respond to those future surveillance threats involved considering how to control overbroad, arbitrary, and invasive surveillance capabilities.[385]

3. Race and Tyranny

A century removed from the Founding, a different sort of tyranny motivated the passage of the Fourteenth Amendment. While the focus in the constitutional text is on equal protection and due process[386]—and the horror of slavery was paramount to its passage—arbitrary and abusive racialized-policing practices also played an important background role. Reconstruction surveillance tactics offer a striking historical parallel in terms of arbitrary and overbroad police powers directed at the African-American community.[387]

The late Professor Andrew Taslitz wrote the definitive history of the Fourth Amendment and the Reconstruction Amendments.[388] In his scholarship, he examines how Southern states responded to abolition and the fight to end slavery with oppressive and intrusive policing practices.[389] Some of these policing powers resembled general warrants in their scope, breadth, and granting of discretionary authority to law enforcement officials. Others involved harsh search and seizure tactics seeking to target abolitionists and those supporting the abolitionist cause.

---

most arbitrary manner, without any evidence or reason. Every thing the most sacred may be searched and ransacked by the strong hand of power.'").

384. *See* Donohue, *supra* note 364, at 1240 ("At the most general level, early American colonists reviled search and seizure on the grounds that they unduly interfered with private life. Colonial enmity extended beyond general warrants to any government entry into the home. Response to such searches tended to be immediate and visceral—not part of an intellectualized objection to promiscuous search."); *see also* Davies, *supra* note 364, at 576–77 ("The Framers sought to *prevent* unjustified searches and arrests from occurring, not merely to provide an after-the-fact remedy for unjustified intrusions. For example, the complaints they voiced about searches concerned the breach of the security of the house. Likewise, the constitutional texts they wrote did not simply seek to provide a post-intrusion remedy or condemn only the actual use of a general warrant; rather, the constitutional texts adopted a preventive strategy by consistently prohibiting even the *issuance* of a too-loose warrant." (footnote omitted)).

385. *See* Gray, *supra* note 367, at 457 ("One of the principal concerns confronting those who met in Philadelphia during the hot summer of 1787 was controlling the newly constituted federal government. Conventioneers harbored particular concerns about the power and authority of the central government and its ability to override protections afforded by state constitutions and the common law.").

386. *See* U.S. CONST. amend. XIV, § 1.

387. *See* Michael Kent Curtis, *The 1859 Crisis over Hinton Helper's Book, the Impending Crisis: Free Speech, Slavery, and Some Light on the Meaning of the First Section of the Fourteenth Amendment*, 68 CHI.-KENT L. REV. 1113, 1117 (1993) ("Republicans invoked rights referred to in the First Amendment (here involving antislavery speech, press, and religion), the Fourth Amendment (involving unreasonable searches and seizures aimed at antislavery activists and publications), and the Eighth Amendment (involving cruel and unusual punishments for opponents of slavery) in the years 1859 to 1866 to criticize state political repression that the 'slave power' aimed at opponents of slavery. In this respect the battle between antislavery and slavery replicated earlier battles for political liberty in which dissenters invoked basic liberties, including criminal procedure guarantees later set out in the American Bill of Rights.").

388. *See generally* TASLITZ, *supra* note 34.

389. *Id.* at 12.

For people subject to these arbitrary (but lawful) grants of government power, their complaints sounded in tyranny. For example, police agents enforced the rules of slavery, including all of the attendant invasions of liberty, privacy, and constant surveillance that came with human bondage.[390] After slavery, police and deputized agents enforced the Black Codes and laws that restricted movement through physical stops and seizures.[391] This resulted in a pattern of police encounters, searches, and kidnappings under legal authority.[392] In parallel to the Founding, states responded to abolitionist dissent with crackdowns and searches seeking to suppress political speech that criticized the practice of slavery.[393] Government power was used in an arbitrary and violent manner to control ideas, movement, and the cause of abolition. Again, similar to the revolutionary complaints of the Founders, the abolitionists faced physical searches, increased surveillance, and arbitrary seizures that restricted movement and intruded on private lives and papers.[394]

This fear of tyranny and police power thus influenced the passage of the Fourteenth Amendment.[395] While minimized in modern understandings of the ratification, protection from police searches and seizures was central to the ideal of constitutional equality. Professor Taslitz wrote, "The Republicans who debated the Fourteenth Amendment understood the close connection among the kinds of rights that the Fourth Amendment protected, free speech and press, and

390. Andrew E. Taslitz, *Respect and the Fourth Amendment*, 94 J. CRIM. L. & CRIMINOLOGY 15, 43 (2003) ("[S]lavery was partly defined by the deprivation of Fourth Amendment interests in freedom of movement, privacy, and property.").

391. Justin S. Conroy, *"Show Me Your Papers": Race and Street Encounters*, 19 NAT'L BLACK L.J. 149, 159 (2006) ("Slavery is closely entwined with the Fourth Amendment's relationship with street encounters. The pass system, which limited the movements of African Americans, gave way to the Thirteenth and Fourteenth Amendments."); Taslitz, *supra* note 34, at 746 ("The Black Codes sought to reinstitute the functional equivalent of slavery by impinging upon Black privacy, property, and freedom of movement. The Codes provided for the arrest and return of Blacks who breached labor contracts with their employers, prohibited Black servants from leaving their masters' premises, and authorized hiring out Black children and Blacks unable to pay vagrancy fines. The Codes made certain conduct criminal for Blacks, but not for Whites." (footnotes omitted)).

392. *See* Taslitz, *supra* note 34, at 747 ("The Codes thus sought to repress Black freedom of movement, privacy, and property as an expression of an intolerable idea of equality."); *id.* at 748 ("The Fourteenth Amendment was partly intended to ensure the constitutionality of the 1866 Civil Rights Act, which effectively outlawed the Black Codes.").

393. *See id.* at 714 ("The drafters of the Fourteenth Amendment were concerned with protecting Republican and abolitionist critics of slavery and of the post-slavery reactionary policies of the Southern regime, whose governments had subjected those critics to abusive searches and seizures to silence dissent."); *id.* at 738 ("The ultimate spread of universal suffrage, the rising public attention to the abolitionist cause, and fear of their own slaves led [antebellum plantation owners] toward an ever-greater hysteria about abolitionist thought. They reacted with repressive measures designed to squelch free speech and press. Unjustified and discriminatory searches and seizures were among their primary weapons for silencing dissenters and promoting citizen ignorance." (footnotes omitted)).

394. *See id.* at 740 ("Repressive searches and seizures were not directed solely at those engaged in blatant political speech. The South had a growing fear of slave revolt and violent retribution.").

395. *See id.* at 749 ("Senator Howard quoted *Corfield v. Coryell* on the Senate floor and listed the 'right to be exempt from unreasonable searches and seizures' among the privileges of national citizenship. There is little serious doubt that the Fourteenth Amendment was meant to ensure the application of the Bill of Rights, including the Fourth Amendment, to the states." (footnotes omitted)).

the nature of free movement and privacy as central aspects of the expression of a message of equality."[396] Thus, the original constitutional guidance against tyranny emerged again in the fight for racial equality in the states.[397] From before the Fourteenth Amendment to the present day, police power and government surveillance has been connected to Fourth Amendment values.

4. A Tyranny Paradigm

Historical parallels provide guidance, but not clear justification, for why society should adopt the tyrant test for new surveillance technologies. Just because one can make a historical connection or two does not mean history should shape analysis. Similarly, reference to constitutional values outside of doctrinal interpretation offers interesting insights but no requirement of fidelity.

Yet, if one is looking for common first principles on which to build agreement around new technologies, looking at existing shared understandings can help. As I argue below, a tyrant test combines both the abolitionist sentiment against police power and the technocratic promise of a way forward to limit, regulate, but not completely ban future police technologies. While a bit oversimplified, the Fourth Amendment was a reaction to the problem of potential tyranny, allowing a limited grant of government surveillance power but only within an interlocking structure to prevent abusive and arbitrary enforcement.[398]

B. THE TYRANT TEST

Because the threat of tyranny comes from those with power (even democratically authorized power), the remedy must respond to that power. Limiting the authority of those allowed to use state power through legislation and legally enforceable rights was one such remedy.[399] Situating power in community institutions with full power to check the otherwise legitimate government (such as juries and grand juries) was another such response.[400] Carving out private areas and personal spaces forbidden to police investigation power was a third.[401] Intriguingly, the early theory of the Fourth Amendment—centered around written restrictions, judicial review, civil tort remedies, juries and grand juries, and substantive search limits—offers a jumping off point for modern-day application to surveillance. The goal here is not to bring the past into the future but to use the past to reimagine a new future.

This Section imagines a tyrant test based on Fourth Amendment values. The tyrant test works on two levels. First, it invites a question that new policing

396. *Id.* at 748.

397. *See id.* ("The Reconstruction Congress meant to halt the designation of Blacks as special targets for various searches and seizures.").

398. *See* Steven I. Friedland, *Of Clouds and Clocks: Police Location Tracking in the Digital Age*, 48 TEX. TECH L. REV. 165, 172 (2015) ("The Fourth Amendment was intended to be a limitation on an organic and developing government, requiring some checks and balances as a regulatory limitation on government while also respecting the division between the public and private spheres.").

399. *See infra* Section IV.B.1.a.

400. *See infra* Section IV.B.1.e.

401. *See infra* Section IV.B.2.

technologies must answer: Can a proposed technology pass the tyrant test? In practical form, this means asking whether a structural-power sharing system has been designed and implemented to curtail the tyrant's potential use of the technology. A technology only passes the tyrant test if the proponent can show that the risks and threats have been mitigated by establishing these structural checks on power. Second, the tyrant test reflects a commitment to legal and political oversight, combining the establishment of formal authorizing legislation, judicial oversight, executive branch limits, community-based institutional checks, and individual rights and remedies.

The tyrant test is neither a judicial test nor a constitutional test. It is a first-principles framing theory that builds off lessons learned by studying the Fourth Amendment as a constraint on government power. Two overlapping themes emerge, focusing on structural protections and substantive limitations. Both themes build off the debates around the original Fourth Amendment as a response to potential tyrannical power.

1. Structural Checks

The Fourth Amendment signifies a structural protection against arbitrary government power.[402] Written into the Constitution—our controlling law—it encodes a distrust of all branches of government.[403] The Fourth Amendment forbids legislatures from granting authority to unreasonably search or seize persons, papers, homes, or effects or to weaken warrant requirements below a probable cause standard.[404] The Amendment restricts executive branch agents from effectuating generalized searches or seizures.[405] And, while the Fourth Amendment requires judicial involvement—a nod to the checks and balances in the system—it also reflects a distrust of those same judges. In the Founding Age, judges were not to be trusted.[406] Thus, as a structural matter, the Fourth Amendment limits government power through a series of interlocking power sources centered on enforceable individual rights. As discussed earlier, the need for such a protection came from the assumption that government (in all forms) would abuse its power,

402. *See* Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 991–92 (1999) ("The language of the [Fourth] amendment appears to have been a direct response to the concerns of political minorities of the time that a federal government would trample the individual rights of those groups or individuals who were held in disfavor. Thus, the amendment operated as a structural protection against unregulated police power." (footnote omitted)).

403. *See* Moran, *supra* note 35, at 959 ("When the Framers drafted the Constitution and the subsequent Bill of Rights, they had in their minds an imperfect and untrustworthy government which, if not kept in check, would disregard fundamental liberties, particularly the liberties of minority groups lacking political power.").

404. *See* U.S. CONST. amend. IV.

405. *See* Donohue, *supra* note 364, at 1322 ("The Founders' concern went beyond the amassing of tyrannical power in one place to the impact such an accumulation of power would have on the separation of powers. General warrants gave power to the executive branch, without constraint on how the power could be used. General warrants amounted to the proverbial fox guarding the hen house.").

406. *See* Travis Christopher Barham, *Congress Gave and Congress Hath Taken Away: Jurisdiction Withdrawal and the Constitution*, 62 WASH. & LEE L. REV. 1139, 1169 (2005) ("[T]he Founding generation viewed the judiciary with great skepticism.").

and only written, enforceable, and individually assertable rights would—collectively—check the potential abuse.[407]

The tyrant test borrows from this cynicism of governmental self-restraint and designs structural protections against new surveillance technologies. It is certainly not enough to trust police, as the Fourth Amendment's design does not trust government power. But it also would not be enough simply to trust laws or policies to restrain government. Those could be, as has been argued by those who favor the trap lens, too easily co-opted and weakened by the powerful. Lawful surveillance abuses were still abusive, and as Professor Thomas Davies has argued, the Fourth Amendment was primarily concerned with restraining future legislative grants of abusive (but lawful) surveillance power.[408] The tyrant test thus goes beyond legislative and technocratic checks to a more holistic system of checks involving interlocking and overlapping powers, individual rights and remedies, and limited grants of authorization, so no branch of government can abuse the power.

a. Legislative Checks

As a structural matter, the tyrant test begins with the principle of negative liberties and the requirement of democratic authorization.[409] Police would only be granted surveillance power by explicit authorizing acts from the legislative branch. Liberty from surveillance would be the norm, and public and democratically accountable authorization in written law would be the only exception. In other words, no surveillance technology would be allowed to be used without specific democratic authorization. This structural limit reinforces separations of power and democratic legitimacy, and it offers a measure of checks on police power.

Practically, this would mean any new technology (for example, predictive policing or facial recognition) would need authorizing legislation granted by a democratically enabled body before use. Unlike the last decade of pilot projects, opaque procurement, and tactical secrecy, new technologies would need to be publicly approved before use, akin to the CCOPS model.[410]

In addition, legislation would establish a series of executive branch, judicial, and community checks, as well as grant enforceable rights of action for breach of the authorizing legislation. These protections, which will be discussed in the next few Sections, are centered in legislative rules.

---

407. *See supra* Section IV.A.1.

408. *See* Davies, *supra* note 364, at 590 ("[The Framers] were concerned about a specific vulnerability in the protections provided by the common law; they were concerned that legislation might make general warrants legal in the future, and thus undermine the right of security in person and house. Thus, the Framers adopted constitutional search and seizure provisions with the precise aim of ensuring the protection of person and house by prohibiting legislative approval of general warrants.").

409. *See* Erwin Chemerinsky, *The Alaska Constitution and the Future of Individual Rights*, 35 ALASKA L. REV. 117, 121–22 (2018) ("It has often been said that the United States Constitution is about negative liberties—prohibitions on what the government can do.").

410. *See supra* Section III.B.1.

b. Executive Branch Checks

Second, all such rules around authorization would be written down and publicized consistent with rule of law principles. Reflecting the insights of a written constitution (although embracing the practicality of technocratic use policies), the tyrant test would also require formal rulemaking and strict use limits via enforceable policies. These limits would be executive branch checks enabled and acted on by executive officials.

The tyrant test embraces all of the earlier discussed technocratic solutions to hold police surveillance technology accountable.[411] For example, to ensure a measure of executive branch self-limitation, formal policies, formal audits, formal accountability measures—like the Seattle CCOPS inspired ordinance—must be built into the regulatory structure at the front end. This would include front-end civil rights and civil liberties audits, which would be publicized and turned into written and enforceable policies. In addition, back-end internal accountability systems must be created. New rules around training must teach the limits of using the new technologies, and certifications around accuracy and effectiveness must be designed from the beginning. Finally, the reporting mechanisms must be internal to police and also reflect outwards to legislative authorizing bodies, community oversight bodies, and the people. Internal police policies without external accountability mechanisms are not sufficient, just like mere technocratic reforms are insufficient. As will be discussed, violations of the policies and internal rules must have remedies via legislative, judicial, community, and individual rights mechanisms.[412] These are not mere reforms around the edges but structural prerequisites for adopting any new technology.

Adding layers of rulemaking is a double-edged sword for accountability. On the one hand, it offers a way to observe, manage, and hold technology to account. On the other hand, the rulemakers concentrate control in the hands of those with power.[413] This type of technocratic solution alone is not enough to control police power, but it does offer a mechanism for transparency, enabling other structural checks, such as lawsuits and community advocacy, to work. For new policing technologies, this would mean that any proposed use must be regulated by public rules, policies, and use restrictions before and after implementation.

c. Judicial Checks

In addition to legislative authorization and executive self-regulation, the tyrant test also requires judicial involvement. Although distrustful of judicial officers, the Founders did envision that courts could play a role to check the other branches

411. *See supra* Sections III.B.1–4.
412. *See infra* Sections IV.B.1.d, IV.B.1.f.
413. *See infra* Section IV.C.

of government.[414] The Fourth Amendment's inclusion of the Warrant Clause acknowledged the judicial role in limiting government power.[415]

The modern Fourth Amendment has relied even more heavily on judicial approval for invasions of liberty.[416] The tyrant test borrows a bit from both old and new approaches. Two separate but related checks are important. One check is that there must be an independent, third-party process for approving surveillance use that sits outside the executive branch. The second check is that the procedural approval must be based on an elevated standard of proof that balances government need and individual liberty in favor of the individual.

First, as to process, the tyrant test would involve a judicial check akin to a warrant for many use cases involving individualized suspicion and surveillance technology.[417] In practical terms, the government would need a signed judicial warrant to conduct a facial recognition search or collect smart data from a targeted person or a third party. The government already follows this probable cause warrant approach before using certain invasive surveillance technologies such as cell site location information tracking, GPS tracking, and Stingray international mobile subscriber identity surveillance.[418] Parallel to the traditional warrant

414. *See* Yanez-Marquez v. Lynch, 789 F.3d 434, 464 (4th Cir. 2015) ("General warrants and writs of assistance bestowed upon the executing officials a high degree of deference and, crucially, 'provided no judicial check' on a judicial officer's determination that an intrusion into a home or dwelling house was justified. The Founders imposed that missing 'judicial check' by adopting the Fourth Amendment, which requires neutral and detached judicial officers to assess whether probable cause has been shown for searches of persons, houses, papers, or effects." (citation omitted) (quoting Steagald v. United States, 451 U.S. 204, 220 (1981))).

415. *See* Davies, *supra* note 364, at 650 ("The common-law sources also shed considerable light on why the Framers objected only to general warrants, but not to specific warrants. At common law, specific warrants provided several layers of protection against arbitrary searches. First, and perhaps foremost, the specific warrant gave a particularized command to the officer, thereby circumscribing the officer's exercise of his own judgment as to whom to arrest, what place to search, or what items to seize. The specific warrant controlled the officer.").

416. *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("Searches conducted without warrants have been held unlawful 'notwithstanding facts unquestionably showing probable cause,' for the Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . .'" (alterations in original) (citation omitted) (first quoting Agnello v. United States, 269 U.S. 20, 33 (1925); then quoting Wong Sun v. United States, 371 U.S. 471, 481–82 (1963))).

417. *See, e.g.*, Thompson v. Louisiana, 469 U.S. 17, 20 (1984) (per curiam) ("[W]e have consistently reaffirmed our understanding that in all cases outside the exceptions to the warrant requirement the Fourth Amendment requires the interposition of a neutral and detached magistrate between the police and the 'persons, houses, papers, and effects' of citizens.").

418. *See* Carpenter v. United States, 138 S. Ct. 2206, 2215, 2221 (2018) (cell site location information); United States v. Jones, 565 U.S. 400, 405–08 (2012) (GPS); United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (international mobile subscriber identity devices) ("[T]he Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator." (first citing Press Release, DOJ, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators (Sept. 3, 2015), 2015 WL 5159600; and then citing Richard Downing, Deputy Assistant Att'y Gen., Dep't of Just., Deputy Assistant Attorney General Richard Downing Testifies Before House Oversight and Government Reform Committee at Hearing on Geolocation Technology and Privacy (Mar. 2, 2016), 2016 WL 806338 ("The department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes."))).

requirement, a formal process to use a new surveillance technology for investigative purposes would require an independent judge to sign off.

An even stronger protection would be to analogize to the authorities of Title III of the Wiretap Act[419] and require a "super warrant" before using a technology. In the facial recognition context, I have previously sketched out how a super warrant (parallel to Wiretap Act requirements) should apply to certain surveillance technologies.[420] In simple terms, authorizing legislation would require police to: (1) obtain judicial approval to use certain liberty-infringing technologies, (2) limit use to serious violent felonies, and (3) rely only on the technology after other non-technological investigation mechanisms have been deemed unhelpful.[421] Mirroring existing Title III Wiretap Act authorization, the tyrant test would require similar police surveillance authorization. While wiretap authorities are not without criticism, involving ever-expanding use and routinized approval, oversight is stronger than standard probable cause warrants or the status quo (of no warrants at all).

The second check involves the requirement of probable cause before the surveillance technology can be authorized via judicial warrant. Warrants without legal standards offer little protection. The constitutional terminology of probable cause (although diluted in recent eras) provides a baseline level of proof to justify an invasion of liberty.[422] The tyrant test would also require at least a probable cause standard to justify police use of any technology. Police would need to assert under oath the rationale for why a certain technology was used in a particular criminal investigation. The probable cause standard is not terribly protective, but it does generate a written record of the ex ante grounds of suspicion and acts as a forcing mechanism to justify use.[423]

---

419. *See* Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. § 2518. Under this federal statutory provision, investigators can ask a judge for a wiretap order to listen to conversations from a suspect's home or cell phone. *id.* § 2518(1). The level of suspicion for a wiretap warrant is probable cause, but investigators must also detail why there are no other alternatives, what will be done to minimize incidental collection, and the time and limits of the proposed collection. *See id.* § 2518(1)(b)–(d), (3)(a)–(b). Wiretap orders must be signed off on by a judge. *Id.* § 2518(3). Because of the invasive nature of the request—receiving permission to listen to the content of personal conversations—the standards are higher than a judicial warrant and taken seriously. The colloquial term *super warrant* signifies the heightened legal standard, seriousness, and limits compared to an ordinary judicial warrant.

420. *See* Ferguson, *supra* note 15, at 1202–07 (suggesting a Wiretap Act-like process for use of some facial recognition matching technology).

421. *Id.* at 1204–05.

422. Andrew Manuel Crespo, *Probable Cause Pluralism*, 129 YALE L.J. 1276, 1279–80 (2020) (discussing the history and puzzle of probable cause).

423. *See* State v. Patterson, 515 P.2d 496, 502–03 (Wash. 1973) ("In a search warrant issued under law by a judicial officer, however, there is more than the protective shield of probable cause. The written record surrounding the judicial issuance of a search warrant probably affords greater protection to the individual against abuse of power by the police than does the generalized requirement of reasonableness and probable cause. The warrant itself is a direct command to the peace officers to proceed circumspectly, to make a record of their actions in executing the search and to make a return to the issuing judge. Thus, the police must serve the warrant within the time specified in it, or within a reasonable time of its issuance or within a time specified by law; they must make a report to the court in writing particularly describing the articles seized and describing the place or persons from whom taken.

A probable cause–warrant approach, however, does not easily fit passive, mass-surveillance technologies that are always collecting data, such as automated license plate readers or video surveillance cameras.[424] One of the problems of new surveillance technologies is that they apply broadly without particularity and collect data continuously. Probable cause—as a standard of individualized suspicion—cannot be met without a particularized target or crime.[425] The consequence of a probable cause requirement for these data collection systems is that it would essentially ban them because, by design, they are never based on individualized probable cause.

The solution—as other scholars have recognized—is to focus on use, not collection.[426] A probable cause requirement to search within the established collection systems could be required by an authorizing statute. Although outside the traditional Fourth Amendment analysis, which focuses on collection and not use, there is nothing preventing enabling legislation from requiring judicial-warrant equivalents for particular use within surveillance systems.[427] So, for example, a probable cause warrant could be required for examining footage within the network of digital surveillance cameras or within the collected license plate database. Investigating officers would need to be able to point to probable cause of a suspected crime (for example, a bank robbery) and probable cause that the dataset will contain useful information (for example, that the license plate of the getaway car is likely in the automated license plate reader dataset). All of these procedures would need to be implemented before use to satisfy the tyrant test. The corollary (and cost) to this requirement is that generalized surveillance using these technologies would almost never be allowed. Generalized use of facial recognition or mass collection of geolocational data—because it has no individualized target or suspicion—would be disallowed. The only use of the technologies would be with a high enough level of suspicion to survive judicial scrutiny and a warrant.

Again, this is not a Fourth Amendment argument for why probable cause warrants are required to use surveillance technology but an analytical model on how

---

These requirements of a written record as a basis for the warrant and a written return to the issuing judicial officer showing exactly what actions were done under its authority probably affords the individual and his house, his papers and his effects conceivably as great a protection from unwarranted police intrusion than the minimal standards of reasonableness mentioned in the constitution.").

424. *See* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 143–84 (2017).

425. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 320 (2016); *see, e.g.*, United States v. Gatto, 313 F. Supp. 3d 551, 560 (S.D.N.Y. 2018) ("The Fourth Amendment mandates 'that a search warrant describe with particularity the place to be searched and the persons or things to be seized.' To be sufficiently particularized, a warrant must, (1) 'identify the specific offense for which the police have established probable cause,' (2) 'describe the place to be searched,' and (3) 'specify the items to be seized by their relation to designated crimes.'" (footnote omitted) (first quoting United States v. Rosa, 626 F.3d 56, 61 (2d Cir. 2010); and then quoting United States v. Ulbricht, 858 F.3d 71, 99 (2d Cir. 2017))).

426. *See, e.g.*, Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 GEO. MASON L. REV. 412, 440 (2018).

427. *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 17–18 (2015).

to structure legislative checks to restrain the metaphorical tyrant. The operating authority is still legislative and regulatory but requires judicial checks.

d. Rights-Based Checks

Fourth, enforceable remedies akin to constitutional rights for surveillance abuses would be included in any authorizing law. In effect, this means granting individual causes of action for violations of controlling laws in the authorizing statutes. Creating affirmative and enforceable legal rights for violations of the authorizing legislation would allow individuals to challenge the technology in court. Even if the existing litigation barriers of cost, time, and expertise exist, a clear remedial mechanism for individual rights with access to the judiciary would act as another check on police power.[428] These rights would allow individuals and communities to sue if the surveillance technology exceeds authorization, violates policy rules, is used to invade constitutional rights under the First or Fourth Amendments, or discriminates on the basis of race.

Rights on paper cannot be protected if legal barriers to court exist. Reasons why litigation has been an unsuccessful check on surveillance include the legal doctrines around standing, immunity provisions, and the cost of litigation.[429] Grants of third-party standing, removal of immunity provisions, and other litigation barriers will need to be addressed in the authorizing legislation.[430]

Rights—enforceable in court without the usual barriers to litigation—need to be front and center of the protections for groups to bring legal challenges. For example, if a surveillance technology were used in violation of an authorizing ordinance or exceeded the grant of authority, the impacted individuals and community institutions should be able to file a lawsuit.[431] The suit could involve an injunction to end the unauthorized use of the technology or monetary damages (or both) and be enforceable via a tort suit. Local jurors might hold police departments to account for misuse of existing grants of power. The tort suit would be similar to the original manner by which Fourth Amendment violations were brought in civil court with civil damages in front of local juries.[432] In fact, the entire logic of the original Fourth Amendment depended on an enforceable civil

428. A good example of this type of legislatively granted right is the Illinois Biometric Information Privacy Act, which allows Illinois citizens to sue for illegally harvested biometric data. 740 ILL. COMP. STAT. 14/20 (2021).

429. This is not to say that there have not been successful lawsuits. Community groups and the ACLU brought a legal suit against the Baltimore Police Department, challenging the use of aerial technology—"planes equipped with high-tech cameras"—in Baltimore. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333 (4th Cir. 2021) (en banc).

430. Each of these barriers to litigation is formidable. The recent debates to modify qualified immunity crystalize how hard it will be to establish legislation that allows individual accountability mechanisms. *See, e.g.*, Joanna C. Schwartz, *Qualified Immunity and Federalism All the Way Down*, 109 GEO. L.J. 305, 307–08 (2020) (discussing the recent proposals to change qualified immunity).

431. The CCOPS draft legislation includes an individual remedies section, providing attorney's fees, whistleblower protection, and other litigation protections. ACLU, *supra* note 277, at 7–8.

432. *See* Amar, *supra* note 364, at 786 ("Tort law remedies were thus clearly the ones presupposed by the Framers of the Fourth Amendment and counterpart state constitutional provisions.").

remedy.[433] This type of plaintiff-friendly legal regime would add legal costs to the surveillance regime. Impacted individuals would sue and likely would regularly challenge misuse of surveillance technology. But the threat of litigation and the individually enforceable suits would offer a mechanism to counterbalance police power. While litigation cannot prevent the abuse of surveillance, it might offer a mechanism to remedy surveillance harms. In addition, in the authorizing legislation, the provision of attorney fees and waivers of traditional government immunity provisions must be included to encourage litigation.

Lawsuits challenging surveillance would not mean that the litigants would win. Lawyers still would have to demonstrate to juries why the misuse was harmful. And traditional juries—old and new—may not be perfect vehicles to implement a tyrant test. That said, the idea of creating a local body of community agents randomly tasked with curtailing the abuses of government power may offer more protection than the technocratic, rule-focused response of elites.

Rights also have a symbolic function of reasserting the power balance desired by society. As part of the tyrant test, this balance favoring individual rights over government surveillance must be reestablished. In any enabling legislation, the individual, collective, and community rights to privacy, liberty, security, and freedom from discrimination must be articulated and given recognition. This declaration of rights in the enabling acts must be publicly stated in ways that reflect the changing power of digital surveillance.[434]

Finally, definitions in these rights-granting laws must expand currently narrow or contested interpretations around digital privacy. For example, much debate has centered around how to reconceive privacy in traditional Fourth Amendment fixtures such as homes, persons, papers, and effects.[435] These physical concepts now have digital analogues, leading to open questions about the scope of protection. Enabling legislation limiting police surveillance can be drafted to incorporate digital equivalents of these constitutionally protected interests and fill the lacuna created by the digital world.[436] Constitutional gaps around issues of collective privacy,[437] fiduciary

433. *See* Davies, *supra* note 364, at 624–25 ("At common law, a search or arrest was presumed an unlawful trespass unless 'justified.' Thus, law enforcement authority as such consisted simply of those justifications for arrests or searches recognized by the common-law treatises and cases. . . . Furthermore, the victim of an unlawful arrest or search could sue the offending officer for trespass damages. The common law recognized no broad doctrine of official immunity." (footnote omitted)).

434. For example, Illinois legislated additional privacy protections for biometric information, some of which is captured by digital surveillance technologies such as facial recognition. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10, 15, 20 (2021).

435. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 552–53 (2017) (exploring the constitutional gaps in Fourth Amendment law).

436. *See id.*

437. *See* David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 79 (2018); David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH L. REV. 189, 191 (2015).

protections,[438] third-party access,[439] and mass surveillance[440] could be addressed at the front end in legislative text. New technologies will raise hard questions that cannot all be answered in enabling legislation, but many gaps have already been identified and could be addressed, including expanded definitions of harms, grants of community standing to sue, and future proofing protections to help with interpretation of how traditional, analog protections should be evaluated in the digital age. What matters is that the tyrant test includes individual and collective legal rights to challenge the tyrant's use of power within the authorizing statute.

e. Local Participatory Checks

Fifth, structures of citizen participation should be created in the authorizing legislation. Local institutions could be given absolute approval power before adopting any technology. This shift to localized control is one of the markers of the tyrant test. The key is decentering power away from the government institutions and reallocating it to the community. This citizen-participation element deserves some exposition because it offers a more fundamental power shift beyond legislative, executive, and judicial checks.

One model for citizen-based institutional limits on government power is the grand jury. At the time of the Founding, grand juries were decentralized checks on government power.[441] Grand jurors were given a whole host of broad quasi-legislative powers to regulate their communities, including initiating investigations and tax collection.[442] Grand juries were not considered an arm of the prosecution but an independent community check to oppose executive power. Similarly, trial jurors played a much more significant role in criminal cases, deciding both law and fact.[443] It was also the civil jury that decided the reasonableness of a government search and thus whether the search was a violation of

438. *See generally* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 649–57 (2015) (laying the groundwork for determining who are Fourth Amendment fiduciaries).

439. *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 378 (2019) (summarizing *Carpenter*'s three-factor test that should be applied based on the category of information being sought, not the specific facts of a case).

440. *See* Rushin, *supra* note 9, at 286–87.

441. Brent Tarter & Wythe Holt, *The Apparent Political Selection of Federal Grand Juries in Virginia, 1789–1809*, 49 AM. J. LEGAL HIST. 257, 260 (2007) ("Grand juries were of equal importance with trial juries. Anglo-American traditions of popular liberty required not only citizen participation in the adjudication of the guilt or liability of their fellows, but also that citizens participate in the process of charging fellow citizens with crimes.").

442. *See* Roger A. Fairfax, Jr., *Grand Jury Innovation: Toward a Functional Makeover of the Ancient Bulwark of Liberty*, 19 WM. & MARY BILL RTS. J. 339, 354 (2010) ("[G]rand juries in colonial America levied taxes, allocated public works spending, appointed government officials, and helped to manage other affairs of local government.").

443. *See* Douglas A. Berman, *Making the Framers' Case, and a Modern Case, for Jury Involvement in Habeas Adjudication*, 71 OHIO ST. L.J. 887, 888, 892 & n.24 (2010) ("[I]t was widely believed in the Framing era that juries could and should have authority to decide matters of both law and fact when rendering a general verdict about a defendant's fate.").

the Fourth Amendment.[444] Therefore, the juror as a citizen and the jury as institution represented the community and had a central voice in controlling government power and checking tyrannical impulses.

Now imagine that before a surveillance technology were adopted, a city had to receive a local institution's approval—the equivalent of a grand jury—made up of local citizens.[445] Twenty-three randomly selected citizens—guided by tech experts, lawyers, and researchers—would approve or disapprove surveillance technologies based on their local views.[446] The geographic areas could be kept small, and different areas of a city might come out with different outcomes.

This democratic approval of policing power would be local—centered on communities impacted by police surveillance, with juries selected from these areas. Whether seen as an example of federalism or a practical acknowledgment of the fragmented, local differences in policing, the locus of authorization must be from the community. Formal civilian oversight boards with final authorizing power and other forms of direct participation would be built into the system of approval and accountability. It could be the case that a networked series of cameras would be allowed in one neighborhood but banned from another. Local groups might make different local choices. This has been the call from some Black Lives Matter activists and others engaged in localizing the process of police reform.[447] Unless approved by a locally constituted authority with authentic community input, police surveillance technologies would not be allowed to operate.

A loose, city-wide model for these community-based oversight bodies can be found in Oakland's Privacy Advisory Commission.[448] As described earlier, the

444. Raymond Shih Ray Ku, *Privacy Is the Problem*, 19 WIDENER L.J. 873, 886 (2010) ("[T]he Founders believed that '"the people,"' and not judges, were 'to protect both individual persons and the collective people against a possibly unrepresentative and self-serving officialdom.' The people exercised considerable power in these preconstitutional cases because juries, not judges, determined the reasonableness of a search." (footnote omitted) (quoting AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 68 (1998))).

445. *See* Adams & Rameau, *supra* note 161, at 530 ("Ending the occupation and initiating truly democratic Community Control over Police in the Black community must manifest in the form of civilian boards, comprised of residents subject to police jurisdiction, with 100%-complete authority over the priorities, policies, and practices of the police. Such boards are essential to realizing the 'consent of the governed,' as the governed would exercise control over those who carry arms and have the right to enforce laws, deny people their freedom, and even, in extreme circumstances, take lives in the name of the governed."); Udi Ofer, *Getting It Right: Building Effective Civilian Review Boards to Oversee Police*, 46 SETON HALL L. REV. 1033, 1044 (2016) (proposing a civilian review board in which the "majority of the board is nominated by civic organizations that have an interest in the safety of the city and in the civil rights of community members" and that has actual disciplinary power).

446. Adams & Rameau, *supra* note 161, at 536 ("A randomly selected board, based on demonstrable residency in the policing district, is vital to advancing the democratic ideal of informed consent of the governed and is the only way to achieve true Community Control over Police.").

447. *See* Akbar, *supra* note 169, at 434 ("The demand for community control is a rejection of the community policing frame. Community control instead posits the problem as one of power and accountability: that Black communities do not have meaningful power or input in how the police forces that govern them operate."); *Community Control*, *supra* note 216 ("We demand a world where those most impacted in our communities control the laws, institutions, and policies that are meant to serve us . . . .").

448. *See supra* notes 301–02.

Oakland Privacy Commission has been a good example of a city-wide community oversight institution with influence.[449] The difference would be that in addition to the appointed commissioners in Oakland—who might reflect interests of lawyers, activists, technologists, or law enforcement[450]—the tyrant test model would also have members of the community selected through a random, jury-like lottery. In fact, the same jury selection system could be used. In addition, unlike the city-wide model, the tyrant test would be more localized, centered in neighborhoods and smaller jurisdictional areas.

The tyrant test version of this type of local oversight-surveillance jury would also balance community interests and expertise.[451] The goal would be to create a mix of technology-informed experts who can address the acknowledged concerns of new technology and ordinary citizens, summoned just like jury duty, who would represent the community. Together—experts and the impacted community—would decide whether to approve any new, legislatively authorized surveillance technology.

If one's reaction to such an embrace of local power is that it is unworkable, inefficient, or debilitating to good governance, the Founders might disagree.[452] In fact, the reason for the grand jury was to make it hard for such government powers to be used, and local criminal juries were explicitly designed as antityranny institutions. Seeing the grand jury and petit jury as this radically localized power center (onerous enough to thwart potential tyranny) is exactly the point.[453] Although co-opted by judicial and prosecutorial power today, the original jury and grand jury were thorns in the side of government power and meant to protect against tyranny.[454] The same role can be played by citizen-based surveillance

449. *See supra* notes 299–309 and accompanying text.

450. The Oakland Ordinance suggests that the commission's membership include a variety of criteria covering the above categories. *See* Oakland, Cal., Ordinance 13349 (Dec. 17, 2015), https://cao-94612.s3.amazonaws.com/documents/Privacy-Advisory-Commission-final-Ordinance-13349-CMS.pdf [https://perma.cc/A4LH-XWAE].

451. *See* Ofer, *supra* note 445, at 1042 (describing how many police oversight boards are "overseen by a review board that is majority nominated and majority appointed by the mayor (or in combination with the head of the police), thus minimizing the independence of such boards").

452. *See* Berman, *supra* note 443, at 893 ("[T]he Framers were eager to create a permanent role for juries in the very framework of America's new system of government. The Constitution's text was intended to make certain that the citizenry could and would serve as an essential check on the exercise of the powers of government officials in criminal cases.").

453. For several examples of parallel ideas of community control over policing, see Akbar, *supra* note 169, at 433 (explaining that community control "includes 'democratic community control' of police, so that 'communities most harmed by destructive policing have the power to hire and fire officers, determine disciplinary action, control budgets and policies, and subpoena relevant agency information'" (quoting *Community Control*, *supra* note 216)); Redmond, *supra* note 162, at 232 ("The current system of police oversight is not working for the benefit of the people. It is working for the benefit of the economic elite. It is time for a paradigm change. It is time to put control of the police in the hands of the people.").

454. *See* Duncan v. Louisiana, 391 U.S. 145, 155–56 (1968) ("The guarantees of jury trial in the Federal and State Constitutions reflect a profound judgment about the way in which law should be

juries when it comes to surveillance technology.[455]

The key to success would be that these community organizations would be given final decisionmaking authority to approve or disapprove the technology. Although these decisions could be reevaluated over time, the decisions would be final until a change. So, even with an authorizing law, judicial checks, and legal rights, the technology could not be implemented if the local citizen-based surveillance juries rejected use in their community.

f. Equal Protection Checks

Sixth, and finally, the legislation would include principles of equal protection to ensure nonracist use of the technology and remedies for breach. Reflecting the animating concerns of the Fourteenth Amendment, these equal protection principles would require preapproval, ex post audits, and remedial legal mechanisms to evaluate disparate impact and effect.

If Fourth Amendment equal protection safeguards were in one measure a response to arbitrary and abusive police power based on racial tyranny, a tyrant test must explicitly address the racial inequity in the use of police technologies. A first step would be to require a form of nondiscriminatory preclearance proof before adoption. Simply stated, a technology would need to show that it does not racially discriminate before adoption. This preclearance process would need to be attuned to race-neutral proxies for racial inequality, but the testing and standards are possible. Facial recognition technology is tested for racial bias by the National Institute of Standards and Technology and other independent organizations.[456] Predictive policing has been tested for possible racial bias inherent in its use.[457] Although not perfect by any means, the capacity to test for racial bias exists.[458]

---

enforced and justice administered. A right to jury trial is granted to criminal defendants in order to prevent oppression by the Government. Those who wrote our constitutions knew from history and experience that it was necessary to protect against unfounded criminal charges brought to eliminate enemies and against judges too responsive to the voice of higher authority. The framers of the constitutions strove to create an independent judiciary but insisted upon further protection against arbitrary action. Providing an accused with the right to be tried by a jury of his peers gave him an inestimable safeguard against the corrupt or overzealous prosecutor and against the compliant, biased, or eccentric judge." (footnote omitted)).

455. *See* Patel, *supra* note 266, at 798 ("Rather than viewing the various methods of police reform as consensus building, legitimizing, or transparency mechanisms, I suggest community engagement elevates the role of stakeholders and affected individuals through a *contested* process. In some circumstances this contestation creates the potential for a shift in power between communities and the police.").

456. *See, e.g.*, PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 1–3 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/WV7R-G8BP]; Buolamwini & Gebru, *supra* note 270, at 8–11.

457. *See generally* Brantingham et al., *supra* note 246 (testing for racial biases using arrest data from a predictive policing experience in Los Angeles).

458. Cathy O'Neil, a national expert on algorithmic fairness and auditing, has created a consulting service to audit for racial and gender inequities. *See O'Neil Risk Consulting & Algorithmic Auditing: It's*

Preclearance is only the beginning. Audits to determine racial impacts and inequities must also be created at the back end. Many well-meaning projects result in unintended, unequal outcomes. As a result, audits must be created in the authorizing legislation to ensure that racial bias does not undermine the fairness of the technology.[459] Finally, remedies within the authorizing statutes must allow equal protection challenges to be bought in court if it could be shown—based on the audits—that the surveillance technology was designed or implemented in a way that demonstrated racial bias.

g. Systemic Checks

Each of these procedural protections could be implemented by legislation. Although modeled on constitutional insights, the enabling power would likely need to be legislative and not constitutionally grounded. In many ways, the tyrant test builds off of the strong version of the technocratic model but with a more cynical starting point and a stronger shift in power toward community institutions and individual rights. If the technocratic approach centers power on the legislature to democratically approve surveillance, the tyrant test centers power on the community to democratically resist surveillance. The end goal would be to create a legislatively enacted but community-based power structure—a practical, interlocking system of checks, rights, and laws that would limit even the worst actor from misusing the technology in an arbitrary or generalized manner.

2. Substantive Limitations on Surveillance Power

Although the procedural parts of the tyrant test build off technocratic-seeming limitations, the substantive parts reflect more abolitionist and trap lens values. Certain types of searches would be prohibited no matter the procedural niceties followed. This substantive limitation also tracks a more traditional understanding of the Fourth Amendment, which restricted certain types of searches of personal papers.[460] Professor Morgan Cloud has written: "The substantive limit precludes searches and seizures of some property, even if the Amendment's procedural requirements are satisfied. Private papers are the archetype of tangible property deserving greater protection than other kinds of property. Papers are special because they contain the physical manifestations of the author's thoughts."[461] Although absent from today's Fourth Amendment debates, the early

the Age of the Algorithm and We Have Arrived Unprepared, ORCAA, https://orcaarisk.com/ [https://perma.cc/22T4-FXPZ] (last visited Oct. 28, 2021).

459. As an example, Congress has proposed bills that would require such data audits. *See, e.g.*, Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (proposed Apr. 10, 2019).

460. Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 620–21 (1996).

461. *Id.* at 620; *see id.* at 620–21 ("*Boyd* and *Weeks* rested in large part on the conclusion that because of the inherent testimonial attributes of papers, the Fourth and Fifth Amendments run together to create a zone of privacy into which the government cannot intrude unless the papers are stolen property, contraband, criminal instrumentalities, or required records—papers in which the government can assert an independent interest, or over which it can assert independent authority.").

understanding of the Fourth Amendment involved a far more privacy-protective vision of government monitoring and surveillance powers.[462]

Again, for our purposes, the references to Fourth Amendment history and theory are offered as a way to develop a tyrant test model of regulatory constraint, not as a constitutional argument. The tyrant test is not the Fourth Amendment, and the Fourth Amendment is not the tyrant test. The point here is that one way to think about reducing police surveillance powers is to recognize that some private areas were once protected from all government monitoring and could be again.[463]

a. Papers and Tyranny

At the outset, it is important to acknowledge that all originalist understandings of the Fourth Amendment are contested.[464] That said, one interpretation of the early cases that inspired the Fourth Amendment suggest a much stronger substantive bar on certain types of government monitoring of papers and ideas.[465] The argument here is not that the Fourth Amendment should be interpreted to bar these types of searches (although perhaps it should) but that a tyrant test modeled on the Fourth Amendment's response to tyranny should protect against these types of invasions.

To go back to the seminal search cases that influenced the drafting of the Fourth Amendment, one thing was clear—certain types of searches were especially concerning. For example, the searches in *Entick v. Carrington*[466] and *Wilkes v. Wood*[467]—two cases that influenced the Founding Generation—were vilified not because they were unauthorized (in fact they were duly authorized) but because of what they sought: the papers and private ideas of individuals.[468]

Much ink has been spilled explaining the influence of *Entick* on the Framers of the Fourth Amendment.[469] The case involved a political dissenter's lawsuit

462. *Id.* at 618–19 ("The text and history of the Fourth Amendment demonstrate that it exists to enhance individual liberty by constraining government power." (footnote omitted)).

463. *See, e.g.*, Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness,"* 98 COLUM. L. REV. 1642, 1646 (1998); William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 561 (1992) ("[I]f Fourth Amendment law is to have any real bite, there must be *substantive* restraints on government power.").

464. *See* Brian Sawers, *Original Misunderstandings: The Implications of Misreading History in* Jones, 31 GA. ST. U. L. REV. 471, 477 (2015) ("The original understanding of the Fourth Amendment is one of the most contested issues in constitutional originalism."); *see also* sources cited *supra* note 364.

465. Cloud, *supra* note 460, at 619 ("The fourth amendment enacts a vision of the individual as an autonomous agent, empowered to act and believe and express himself free from government interference.").

466. (1765) 95 Eng. Rep. 807 (KB).

467. (1763) 98 Eng. Rep. 489 (KB).

468. *See* Donohue, *supra* note 364, at 1198 (discussing *Entick v. Carrington*: "[I]t was not the physical break-in or the rummaging in drawers that constituted the essence of the Crown's misconduct, but rather the invasion of the indefeasible rights of personal security, liberty, and private property. Every man in his home was entitled to live free from the gaze of the Crown. The right to privacy ought not to be infringed. The wrong occurred not just when property was confiscated or incriminating evidence obtained, but at the moment the King's messengers entered." (footnote omitted)).

469. *See* T.T. Arvind & Christian R. Burset, *A New Report of* Entick v. Carrington *(1765)* 2 (Notre Dame Legal Stud., Paper No. 200131) ("The Supreme Court has described [*Entick*] as 'the true and

against the government officials who ransacked his home looking for written proof of his seditious complaints.[470] Lord Camden's condemnation of this search influenced American revolutionaries who wished to protect their own dissenting views from future government overreach.[471] *Entick* suggests that surveillance of private ideas should be prohibited regardless of warrant procedures and well-founded suspicion.[472] Simply stated, it was the search that was condemned, independent of the legal justifications and authorities. Even if treasonous, even if criminal, the papers of *Entick* or *Wilkes* were not to be exposed to government eyes, even with a particularized warrant.[473]

These cases influenced American lawyers who drafted the Fourth Amendment.[474] The harm that the Fourth Amendment was supposed to protect against was government surveillance of private ideas in protected spaces such as homes. It was not just the harm of confiscating the papers or rummaging through private spaces but also the threat to liberty of monitoring private lives.[475]

The Supreme Court's first significant Fourth Amendment case reaffirmed this privacy-protective view. In *Boyd v. United States*, the Supreme Court held that a government court order for business records violated the Fourth Amendment.[476] The Court determined that such an invasion into private papers (specifically, in that case, business records) violated the spirit of *Entick* and thus the Fourth

ultimate expression of constitutional law' for the Founding generation, a case that not only illuminates the Fourth Amendment but helped to inspire it." (footnote omitted) (quoting Boyd v. United States, 116 U.S. 616, 626 (1886))); Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 104 (2013) ("American courts recognized *Entick* as part of the received body of English common law.").

470. *See Entick*, 95 Eng. Rep. 807.

471. *See* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 985–87 (discussing *Entick*).

472. *See* William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 399 (1995).

473. *See* Clancy, *supra* note 471, at 987 ("Camden also rejected the government's ability to search papers as a means of discovering evidence in either criminal or civil cases. To emphasize the strength of that substantive restriction on the government's ability to search, he said: 'yet there are some crimes, such for instance, as murder, rape, robbery, and house-breaking, to say nothing of forgery and perjury, that are more atrocious than libeling. But our law has provided no paper-search in these cases to help forward the conviction.'" (footnote omitted) (quoting *Entick*, 95 Eng. Rep. 807)); Arvind & Burset, *supra* note 469, at 31 ("For authors who opposed those warrants, the key danger was not the brief trespass they enabled but the more enduring damage they might inflict by exposing the secrets of the government's critics.").

474. *See* Carpenter v. United States, 138 S. Ct. 2206, 2264 (2018) (Gorsuch, J., dissenting) (recognizing that "[t]he Fourth Amendment came about in response to a trio of 18th century cases," including *Entick*); City of West Covina v. Perkins, 525 U.S. 234, 247 (1999) (Thomas, J., concurring in the judgment) (stating that *Entick* "profoundly influenced the Founders' view of what a 'reasonable' search entailed").

475. Morgan Cloud, *Property Is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 54–55 (2018) ("Seizing all of a person's papers then exposing them to scrutiny by others was a particularly odious transgression because papers were a unique form of property. . . . Reading the contents of papers was worse than a physical trespass because reading ideas contained in private papers enabled searchers to invade the writer's mind. Value attached not to the physical paper but to the intangible thoughts expressed in written language.").

476. *See* 116 U.S. 616, 622 (1886).

Amendment.[477] As Professor Donald Dripps has written, the *Boyd* Supreme Court included members who had breathed the same air as the Founders[478] and who were legal historians of the Founding Age.[479] Their reliance on *Entick*, and application of the Fourth Amendment to private papers, shows how broadly the original Fourth Amendment swept to protect the privacies of life.[480] *Boyd* thus reaffirmed that certain types of government surveillance into private spaces, including private papers, were off-limits to government actors (even with legal authority).[481]

This substantive search limitation has been ignored for almost a century and holds little currency in the modern Supreme Court.[482] But such substantive limitations on what could be searched were a part of the original understanding shaped by a fear of tyranny.[483] This was so, not because Colonial-Era surveillance was unable to discover the offending materials but because liberty principles prohibited collection in the first place (even in the face of suspected treasonous activity).[484] Papers recording private ideas, religious beliefs, and dissenting views

477. Sklansky, *supra* note 364, at 1740 ("Justice Bradley's majority opinion in *Boyd v. United States*, the Court's first major interpretation of the Fourth Amendment, drew broad lessons from the eighteenth-century controversies in England and America to which the Amendment responded.").

478. Dripps, *supra* note 469, at 102–03 ("The *Boyd* majority should not be dismissed too lightly. For one thing, the opinion was written less than a century after the ratification of the Fourth Amendment. The Justices had walked the earth with the Founding generation.").

479. *Id.* at 103 ("[O]ne of the members of the *Boyd* majority was Horace Gray, a legal historian who compiled the first archive of primary sources related to the Writs of Assistance controversy.").

480. *Boyd*, 116 U.S. at 630 ("The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employés of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence,—it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.").

481. Cloud, *supra* note 475, at 51 ("[*Boyd*] implemented robust protections for private papers that amounted to a ban on most searches for papers. This special treatment of papers was not a nineteenth century innovation by the Court. It was derived from English cases decided a decade before the Revolution that had influenced ideas about unreasonable searches and seizures in America during the founding period and after.").

482. *See* Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 37 (1986) (noting that the Court rejected *Boyd* in terms of subpoenas).

483. *See* United States v. Hunt, 505 F.2d 931, 936 (5th Cir. 1974) ("*Boyd* was an affirmation of the principle that some things cannot be searched or seized regardless of whether a proper procedure is followed, that a search of private papers is *per se* an 'unreasonable search.'").

484. Donohue, *supra* note 364, at 1307 ("In 1868, Thomas Cooley, chief justice of the Michigan Supreme Court, reiterated the importance of the Fourth Amendment's prohibition on using a warrant to obtain evidence of guilt. Further, he noted: '[F]ound also in many State constitutions, [the Fourth Amendment] would clearly preclude the seizure of one's papers in order to obtain evidence against him; and the spirit of the fifth amendment—that no person shall be compelled in a criminal case to give evidence against himself—would also forbid such seizure.'" (alterations in original) (footnote omitted) (quoting THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 431 n.4 (Victor H. Lane ed., 7th ed. 1903))).

were to be protected even in the face of lawful and procedurally sound search authority.

This is not to say that the Fourth Amendment was an absolute ban on all searches or seizures[485] but only that it was much more skeptical of government search power than modern cases hold. The point of this Article is that this skeptical understanding should guide the tyrant test. This skepticism directly implicated judges whom the Founders presciently feared would legitimate privacy-invasive searches.[486] This skepticism implicated legislatures likely to overreach in power.[487] And the skepticism directly targeted the enforcers, the existing law enforcement agents.[488] These precursors to today's police were neither trusted nor trustworthy.[489] While we have lost this understanding of the Fourth Amendment today, the scope of the original Fourth Amendment suggests a more skeptical and radical view that prohibits governmental collection of private information, including use of new policing technologies.

b. Data and Tyranny

A tyrant test, thus, would carve out certain areas that could not be searched, seized, or monitored, no matter the legal authorization. Specifically, private papers, including digital papers in the home, could be simply inaccessible to law enforcement surveillance, even with a warrant.[490] Going one step further, this limit also could include not just physical or digital papers but the data revealed from constitutionally protected things—homes, effects, and persons. As smart objects reveal more of our patterns, questions, and habits, the private information becomes more akin to revealing our thoughts and beliefs. As I have written previously, the informational security in constitutionally protected interests should

485. *See* Dripps, *supra* note 469 ("[E]ven under the rigid rule of *Boyd* it was 'reasonable' to seize stolen papers, obscene books, and criminal libels.").

486. *See* Davies, *supra* note 364, at 561 (recognizing the irony that the colonial court upheld the writs of assistance case argued by James Otis).

487. *See id.* at 590 (recognizing that the Framers were concerned with legislative grants of power like the general warrant).

488. *See id.* at 578 ("The common-law tradition viewed any form of discretionary authority with unease — but delegation of discretionary authority to ordinary, 'petty,' or 'subordinate' officers was anathema to framing-era lawyers.").

489. *See id.* at 577–78 ("[T]he Framers' perception of the untrustworthiness of the ordinary officer was reinforced by class-consciousness and status concerns. It was disagreeable enough for an elite or middle-class householder to have to open his house to a search in response to a command from a high status magistrate acting under a judicial commission; it was a gross insult to the householder's status as a 'freeman' to be bossed about by an ordinary officer who was likely drawn from an inferior class."); Stoughton, *supra* note 163, at 122 ("Elected sheriffs and constables were the face of public law enforcement, but neither was particularly attractive. 'Corruption . . . was quite common, with sheriffs accepting bribes from suspects and prisoners, neglecting their civil duties, tampering with elections, and embezzling public funds.'" (alteration in original) (quoting KRISTIAN WILLIAMS, OUR ENEMIES IN BLUE: POLICE AND POWER IN AMERICA 32 (2007))).

490. *See* City of West Covina v. Perkins, 525 U.S. 234, 247 (1999) (Thomas, J., concurring in the judgment) (recognizing Lord Camden's extreme position).

extend to when our homes, effects, and bodies generate protected data streams.[491] Such protections may become even stronger when the substance of the protection concerns family matters, political views, religion, or other liberty or autonomy values. The argument here is that although scholars (including myself) have argued that the Fourth Amendment's protections should extend to these digital analogues of physically private spaces,[492] a legislative ban could obviate the need for Fourth Amendment interpretation. Simply stated, legislatures could carve out certain private areas beyond the scope of government surveillance or acquisition.

It is beyond the scope of this Article to describe the extent of substantive limitations, but the goal here is to recognize that some substantive limitations would be consistent with a tyrant test inspired by the Fourth Amendment. For example, smart devices recording questions asked in our homes or monitoring our intimate habits or documents stored on home computers and smartphones could simply be carved out as completely protected—despite the potentially incriminating evidence involved. If precolonial treason (as in *Entick*) is the starting point for protected ideas, the bar is high for justifying government intrusion into private documents. This change in existing practice is radically privacy-protective and likely anathema to law-enforcement interests. But the Founding Generation were radicals when it came to thwarting tyranny and would have questioned police reading their virtual diaries, rummaging through their electronic papers, and if they could have envisioned it, listening in on conversations and activities in their homes.[493] Determining where the lines are drawn around the areas that should be completely off-limits is admittedly difficult, but raising the issue of substantive carveouts is important. Some types of invasive technologies may simply be banned because they would involve the surveillance of personal beliefs, ideas, writings, and views on politics family, or religion—independent of the cost to law enforcement interests.

C. LIMITS ON THE TYRANT TEST

The tyrant test can be criticized as being both under and overprotective. On the one hand, the trap lens advocates might criticize the tyrant test as just being a stronger technocratic approach with a few more interwoven rights and remedies but still subject to the same structural power problems.[494] After all, community oversight over police surveillance concedes the necessity of police surveillance.[495]

---

491. *See* Ferguson, *supra* note 435, at 551 (discussing whether a warrant should be required to obtain this data).

492. *See id.*

493. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791, at 601–782 (2009) (providing an example where a Son of Liberty opposed searches because they subjected "our bed chambers" to "the brutal tools of power," exposing "[the] most delicate part of our families . . . to every species of rude or indecent treatment" (quoting *A Son of Liberty*, N.Y. J. & WKLY. REG., Nov. 8, 1787, at 3)).

494. *See* VITALE, *supra* note 24, at 30.

495. *See Reformist Reforms vs. Abolitionist Steps in Policing*, *supra* note 213 (stating that pushing for community oversight boards "further entrenches policing as a legitimate, reformable system, with a

In fact, almost every trap lens criticism of the trust and technocratic approach can also be leveled at the tyrant lens. It is definitely stronger medicine—but not a cure.

On the other hand, the trust lens advocates will complain that the restrictions are too onerous and police innovation will stagnate as a result. This claim is accurate. Looming litigation and additional requirements to report, audit, and educate will create significant roadblocks to efficiency. Equally difficult, including ordinary citizens in complex policy decisions will interject uncertainty, inconsistency, and delay. Finally, and unquestionably, those seeking to slow adoption or limit use of technology will resort to litigation and community pressure to stop the surveillance. Even the technocratic requirements of surveillance oversight will be weaponized in practice. These costs of avoiding tyranny are real, and the tyrant test accepts them as necessary to avoid the dangers inherent in the surveillance technology.

Others might critique the Fourth Amendment, which has been an imperfect guarantor of personal liberty. The lessons of the last two centuries are filled with examples of police abuse, failed police reforms, eroded privacy, and unchanging police–citizen power all under the authority of existing Fourth Amendment law.[496] Some trap lens advocates might rightly question why relying on a failed legal principle would offer any hope for a different result now. These are fair critiques and can go deeper. Even the original Fourth Amendment left out many people from its protective theory.[497] Those without the education, status, or political power to challenge government invasions through tort law were left without a remedy. Those without privilege or legal status were excluded. These are legitimate critiques without clear responses, except for the argument that the Fourth Amendment analogy offers a path for possible improvement on admittedly unstable ground. In the end, policing power will be reduced with multiple levels of democratic and popular approval required.

Finally, some might even challenge using the U.S. Constitution itself as a framework because of the racial, gender, and class compromises that infected the original American compact.[498] Constitutional protections in the face of constitutional failings may not be the right goal. This too is a fair criticism because constitutional rights have remained more aspirational than actual for far too many people. A constitutional system that began unequal and birthed a country that has remained unequal in terms of race, gender, and economic status may be unable to

'community' mandate" and that "[s]ome boards, tasked with overseeing them, become structurally invested in their existence").

496. *See generally* Akbar, *supra* note 169 (contrasting the DOJ's Ferguson and Baltimore reports with the Vision for Black Lives, and discussing the different conceptualizations of the problem of policing and approaches to reform).

497. *See* Davies, *supra* note 364, at 577–78 (detailing the class bias in the original Fourth Amendment that protected higher status men over everyone else).

498. *See* Roberts, *supra* note 161, at 122 ("On the one hand, there is good reason to renounce the Constitution because constitutional law has been critical to upholding the interests of the racial capitalist regime while advancing legal theories that justify its inhumanity. On the other hand, there is utility in demanding that the Reconstruction Constitution live up to the liberation ideals fought for by abolitionists, revolutionaries, and generations of ordinary black people.").

escape these structural power imbalances. For many in America, the tyranny never lifted but only shifted to other forms of social control and monitoring. Depending on one's privilege within the political, cultural, social, and economic system, this promise of escaping tyranny may never be realized.

Despite these fair criticisms, the tyrant test offers a first-principles path forward. Viewed carefully, the tyrant test blends insight from the trap and technocratic lenses to provide a compromise that might allow some new surveillance technologies to be used with careful (perhaps even onerous) regulation. More importantly, the center of power would shift from the police (and even the government) to the community and the people. While imperfect and reliant on individuals to use the tools to resist power, so too is the Constitution and American democracy. The hope is that the tyrant test can provide a more protective theory for a first-principles debate about the way forward.

CONCLUSION

After a decade of experimenting with big data policing, the time has come for a new first-principles approach. Fearing the metaphorical tyrant offers an appropriate starting point for debate. The risks are real, and the way society approaches the rise of new privacy-destroying technologies is critically important to the future power balance between the police and the people.

Moreover, as discussed, the tyrant test improves upon existing practices. The trust test has failed to address the growing concerns of new surveillance technologies and police misuse of power. Similarly, the trap lens may err too much on the side of disallowing any digital evolution, even technology that might not provide an enhancement of police power. And although the technocratic test offers a workable improvement, it fails to grapple with the structural power dynamics that make internal reforms too weak a response to the growing surveillance threat.

This Article has argued for the tyrant test as a new model to address growing police surveillance. By borrowing from Fourth Amendment history and modeling constitutional principles to emphasize interconnected structural protections, rights, remedies, community participation, equality, and limited enumerated grants of policing power, a system of democratically based, community-centered oversight can be created to allow the use of some surveillance technologies and not others. More importantly, a conversation about how to move the debate forward will share common first principles.