

POLICING POLICE TECH: A SOFT LAW SOLUTION

Barry Friedman[†], *Farhang Heydari*^{††}, *Max Isaacs*^{†††} & *Katie Kinsey*[‡]

ABSTRACT

Policing agencies are undergoing a rapid technological revolution. New products—with almost unfathomable capacities to collect, store, monitor, and transmit data about us—constantly are coming to market. In the hands of policing agencies, some of these products may promise real benefits to society. But too often these public safety benefits are unproven. And many of these products present real harms, including risks to privacy, freedom of speech, racial justice, and much more. Part of “public safety” is being safe from these harms as well.

Despite these risks, new policing tech products continue to be adopted and deployed without sufficient (or any) regulatory guardrails or democratic oversight. Legislative bodies are reluctant to adopt traditional “hard law” regulation. And because there is no regulation, what we are left with is a “race to the bottom” in which policing technology vendors develop increasingly intrusive products with minimal or no safeguards.

This Report explores a “soft law” approach to dealing with the race to the bottom around policing technologies. Specifically, it examines the viability of an independent certification body—governmental or not-for-profit—that would perform both an efficacy review and an ethical evaluation of vendors’ policing technology products, assessing them along privacy, racial justice, and civil rights and liberties dimensions, among others. It explains how, in theory, certification can overcome some of the obstacles facing hard law regulation. It then discusses the practical design considerations that a policing tech certification system would have to navigate. It also surveys the challenges posed in the implementation of a certification regime, including how to ensure the body is legitimate and obtains stakeholder buy-in, and whether certification would encourage or undercut hard law regulation. Ultimately, the Report

DOI: <https://doi.org/10.15779/Z38M90242H>

© 2022 Barry Friedman, Farhang Heydari, Max Isaacs & Katie Kinsey.

† Jacob D. Fuchsberg Professor of Law, Affiliated Professor of Politics, and Founding Director, Policing Project, New York University School of Law.

†† Executive Director, Policing Project, New York University School of Law.

††† Staff Attorney, Policing Project, New York University School of Law.

‡ Staff Attorney, Policing Project, New York University School of Law.

For their many helpful comments and suggestions, we are grateful to our convening participants, Elizabeth M. Adams, Meredith Broussard, Richard Vorder Bruegge, Brandon Buskey, Albert Fox Cahn, Rumman Chowdhury, Cynthia Conti-Cook, Laura Cooper, Catherine Crump, Mary D. Fan, Lori Fena, Joe Ferguson, Andrew Guthrie Ferguson, Christopher Fisher, Jerome Greco, Daniel Kahn Gillmor, Donald Gross, Brian Hofer, Yasser Ibrahim, Lassana Magassa, Ben Moskowitz, Alex Pasternack, Fabian Rogers, Ravi Satkalmi, John Singleton, Mona Sloane, Danyelle Solomon, Vincent Southerland, Katherine Jo Strandburg, Suresh Venkatasubramanian, Doron Weber, Rebecca Ulam Weiner, Michael Wilt, Deborah Witzburg. For their invaluable insight, we additionally are grateful to the various stakeholders we interviewed for our research. For their research assistance, we also thank Brandon Vines, and Nick Tonckens. This work was produced with the generous support of the Alfred P. Sloan Foundation.

concludes that although adopting a certification scheme presents challenges, the idea has enough merit to receive serious consideration as part of a unified system of getting policing technologies in check.

TABLE OF CONTENTS

I.	INTRODUCTION	703
II.	DEFINING THE PROBLEM	708
A.	THE POLICING TECH LANDSCAPE: WIDESPREAD USE, UNQUANTIFIED BENEFITS AND HARMS.....	708
B.	THE ACCOUNTABILITY GAP	713
1.	<i>The current hard law landscape.....</i>	713
a)	The limited constraints of constitutional judicial review	713
b)	Current legislative approaches: few and far between	714
c)	Administrative body regulation: exceptions rather than rule	716
2.	<i>Obstacles facing hard law regulation of policing technology</i>	717
a)	Pacing Problem.....	717
b)	An Information Gap.....	718
c)	An Expertise Gap.....	719
d)	A Public Choice Problem	719
e)	Federalist Fragmentation	720
C.	THE RESULTANT RACE TO THE BOTTOM	721
III.	PRODUCT CERTIFICATION AS PART OF THE SOLUTION? ..	722
A.	WHAT WE'RE EXPLORING	722
B.	COMMON CERTIFICATION EXAMPLES.....	723
C.	CERTIFICATION FOR POLICING TECHNOLOGY: ABSENCE AND DEMAND.....	724
D.	CERTIFICATION AS AN ANSWER TO KEY POLICING TECHNOLOGY GOVERNANCE CHALLENGES	727
1.	<i>Supplying Information and Expertise to Foster Democratic Accountability.....</i>	727
2.	<i>Evading Hard Law Challenges to Curb the Race to the Bottom.....</i>	728
E.	THEORIES OF CHANGE	729
IV.	DESIGN CHOICES.....	731
A.	PRESCRIPTIVE VS. DESCRIPTIVE.....	731
B.	EVALUATING EFFICACY	735
C.	"USE" CASES	739
1.	<i>Don't address use cases.....</i>	740
2.	<i>Certify products, addressing use cases indirectly through product design....</i>	740

3. <i>Directly certify use cases</i>	741
D. SUBSTANTIVE DESIGN STANDARDS	742
E. INSTITUTIONAL DESIGN OF CERTIFICATION ENTITIES	744
F. PUBLIC OR PRIVATE	746
V. CHALLENGES	748
A. GAINING LEGITIMACY AND CREDIBILITY: PUBLIC BUY-IN	748
B. ACHIEVING UPTAKE: AGENCY AND VENDOR BUY-IN	749
C. COMPLIANCE AND ENFORCEMENT	751
D. FENDING OFF REGULATION	752
E. NORMALIZING TECHNOLOGIES	754
F. CREATION OF A CERTIFICATION MARKET	755
VI. CONCLUSION	755

I. INTRODUCTION

Deep below Piccadilly Circus, beyond a maze of underground corridors, lies the Westminster CCTV Control Room. A wall of television monitors offers visitors an intimate view of London city life, from the tony boulevards of Belgravia to the bustling streets of Chinatown. With a few clicks, operators can rotate the cameras 360 degrees and zoom nearly 250 feet; the cameras can even detect the movement of a package inside of a car from three blocks away.¹

Martin O'Malley was impressed. Like thousands of other officials from around the world, the Mayor of Baltimore had made the pilgrimage to London to observe one of the most advanced CCTV systems in existence, in one of the most surveilled cities in the world. The previous year, 2003, Baltimore City had recorded over 11,000 violent crimes, making it the seventh most violent city in the United States.² O'Malley had a problem, and the Brits, it seemed, had hit upon a solution.

The idea was simple. CCTV would serve as a “force multiplier”—a single operator in a CCTV control center could perform the work of many police officers, surveilling multiple neighborhoods simultaneously.³ Moreover, the

1. See Paul Lewis, *Every Step You Take: UK Underground Centre That Is Spy Capital of the World*, THE GUARDIAN (Mar. 2, 2009), <https://www.theguardian.com/uk/2009/mar/02/westminster-cctv-system-privacy>; John Buntin, *Long Lens of the Law*, GOVERNING (Mar. 24, 2010), <https://www.governing.com/archive/long-lens-of-the.html>.

2. See NANCY G. LA VIGNE, SAMANTHA S. LOWRY, JOSHUA A. MARKMAN, ALLISON M. DWYER, URBAN INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION 23(2011), https://www.urban.org/sites/default/files/publication/27556/412403-evaluating-the-use-of-public-surveillance-cameras-for-crime-control-and-prevention_1.pdf.

3. *Id.*; see Buntin, *supra* note 1.

visibility of the cameras would serve as a deterrent to would-be offenders. Announced in 2005, Baltimore's "CitiWatch" program would become one of the most ambitious CCTV programs in the United States.

Any new surveillance system courts some controversy, but officials had a plan. They held a series of public hearings, assuring citizens that the new cameras would be used judiciously. The Baltimore Police Department implemented a new electronic surveillance policy governing the use of technologies like CCTV. These efforts helped earn the buy-in of Baltimore residents, many of whom initially expressed concern that the CitiWatch program would infringe on their privacy.⁴

As democratic engagement around police surveillance goes, so far so good.

Then came Freddie Gray. The 2015 death of a 25-year-old Black man in the back of a police van sparked protests across the city. In the ensuing civil unrest, 350 businesses were damaged, 150 vehicles were set ablaze, and over a hundred police officers were injured. The Baltimore Uprising, as it came to be known, culminated in "the most extensive rioting in Baltimore since the 1960s."⁵

Soon after, local aviation enthusiasts began noticing planes making "strange flight orbits" over Baltimore.⁶ These planes, it would later be learned, were equipped with powerful cameras capturing detailed imagery of the city from above. It was the latest evolution in the CitiWatch program—one that would afford the Baltimore Police Department unprecedented surveillance capabilities. Armed with both ground and aerial cameras, analysts could now identify potential suspects and track their movements across the city with precision.⁷ The planes, which flew for up to ten hours a day, were used by police to investigate everything from property thefts and shootings to unlicensed dirt-bikers.⁸ The public was told none of this.

4. See LA VIGNE ET AL., *supra* note 2, at 23–25.

5. See Marshall Greenlaw, *Baltimore Protests and Riots, 2015*, BLACKPAST (Dec. 17, 2017), <https://www.blackpast.org/african-american-history/baltimore-protests-and-riots-2015-2>.

6. See 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>.

7. See BARRY FRIEDMAN, FARHANG HEYDARI, EMMANUEL MAULEÓN & MAX ISAACS, CIVIL RIGHTS AND CIVIL LIBERTIES AUDIT OF BALTIMORE'S AERIAL INVESTIGATION RESEARCH (AIR) PROGRAM 1–2 (2020), [https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5fc290577acac6192a142d61/1606586458141/AIR+Program+Audit+Report+vFINAL+\(reduced\).pdf](https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5fc290577acac6192a142d61/1606586458141/AIR+Program+Audit+Report+vFINAL+(reduced).pdf).

8. See Reel, *supra* note 6.

The existence of the spy planes became public in August 2016, when journalists published an exposé.⁹ Outrage ensued. The American Civil Liberties Union (ACLU) quickly issued a press release assailing the program as “a privacy nightmare come to life.”¹⁰ Congressman Elijah Cummings pledged to review the program and described its secret nature as “concerning.”¹¹ Said one city councilman, more bluntly: “The [police] commissioner keeps talking about transparency, but every time we turn around, there’s something else where we’re left on the outside.”¹² For its part, the Baltimore Police Department claimed that they did not disclose the aerial surveillance because it was merely an extension of the existing CitiWatch program.¹³ The flights soon were scuttled, but not before a public castigation of the Baltimore Police Department that further alienated it from the community it was sworn to protect.

Baltimore residents were the latest victims of function creep in policing technology. Without any laws on the books to prevent this expanded use of CitiWatch—or even provide the public with basic transparency around this use—legislators were left playing catch up to address violations of their constituents’ civil rights and liberties.

That policymaking is failing to keep pace with advances in surveillance technology has achieved the status of cliché. New innovations proliferate at a dizzying rate, rendering existing safeguards ineffective. Laws regulating these new products are few and far between—unsurprising because lawmakers themselves often lack the most basic information about the technologies that police use. This regulatory gap invites a race to the bottom among vendors

9. *See id.*

10. *See Police Secretly Put Large Part of Baltimore Under Constant Aerial Video Surveillance*, ACLU (Aug. 24, 2016), <https://www.aclu.org/press-releases/police-secretly-put-large-part-baltimore-under-constant-aerial-video-surveillance>.

11. *See* Luke Broadwater & Doug Donovan, *Baltimore City Council Plans Hearing on Undisclosed Police Surveillance Plane Program*, BALT. SUN (Aug. 25, 2016), <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-surveillance-folo-20160825-story.html> [<https://web.archive.org/web/20210705134719/https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-surveillance-folo-20160825-story.html>].

12. *See* Luke Broadwater & Doug Donovan, *Baltimore City Council Plans Hearing on Undisclosed Police Surveillance Plane Program*, THE BALT. SUN (Aug. 25, 2016), <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-surveillance-folo-20160825-story.html>.

13. *See* Brandon Soderberg, *Persistent Transparency: Baltimore Surveillance Plane Documents Reveal Ignored Pleas to Go Public, Who Knew About the Program, and Differing Opinions on Privacy*, BALT. SUN (Nov. 1, 2016), <https://www.baltimoresun.com/citypaper/bcp-110216-mobs-aerial-surveillance-20161101-story.html> [<https://web.archive.org/web/20210824223340/https://www.baltimoresun.com/citypaper/bcp-110216-mobs-aerial-surveillance-20161101-story.html>].

who manufacture and sell new and ever more intrusive surveillance tools to willing policing agencies, often with little proof of their benefits. When these programs inevitably come to light, they engender widespread outrage, distrust, and calls for accountability. Then the cycle begins anew.

As the Baltimore example illustrates, this system serves neither police nor the public well. “Hard law”—what we think of as law: statutes, regulations, and the like—is failing to keep the growth of surveillance and policing technologies in check.

In response to this logjam, the authors—lawyers at the Policing Project, a non-profit center at New York University School of Law—began a project to explore a “soft law” alternative: a certification system for policing technologies. The Policing Project is dedicated to making policing more transparent, equitable, and democratically accountable. Concerned by the unregulated use of technology by policing agencies, we sought and obtained a grant from the Alfred P. Sloan Foundation to study the value in a certification scheme for policing technologies. We studied the matter for the better part of a year, reading all the literature we could lay hands on and consulting numerous experts. Then we vetted the idea by convening relevant experts and stakeholders. All told, we spoke with over 50 people for our research, with equal participation from civil society, government, and industry.

A certification is a type of trademark that tells consumers that a product has met a particular standard. This form of “soft law” governance leverages market forces to promote a particular goal that is traditionally ignored or undervalued in the marketplace.¹⁴ Certification schemes are ubiquitous—if you’ve ever watched a “Rated R” movie, bought “Fair Trade” coffee, or purchased an “Energy Star” appliance, you’ve seen certification in action.

Our idea was that a certification scheme could perform a review of a technology’s efficacy and an ethical evaluation of its impact on civil rights, civil liberties, and racial justice. This, we surmised, would provide vital insights to policymakers and the public and perhaps even motivate the enactment of “hard law” (that is, statutes and regulations). Moreover, certification could create a market for policing products that are more protective of civil rights and civil liberties. And certification might address how products are actually *used* on the ground—Baltimore’s CitiWatch cameras, for example, might be

14. See POOJA SETH PARIKH, ENV’L L. INST., HARNESSING CONSUMER POWER 1 (2003), <https://www.eli.org/sites/default/files/eli-pubs/d13-05a.pdf>.

certified for use as traditional CCTV devices but not as part of an aerial surveillance system.¹⁵

Of course, certification is not without its normative challenges. Certification systems raise concerns about democratic legitimacy—most standard-setters and certifiers either are several steps removed from direct democratic processes or are entirely separate from them. Convincing policing agencies and technology vendors to adopt a certification scheme would be no small feat, and the threat of industry capture is an ever-present concern.

These points are well-taken but not insurmountable. As our Report explains, careful design and a set of institutional safeguards can help to ensure that certification is independent, responsive to public concerns, and valuable to lawmakers, vendors, and police alike. Whether a certification regime would accomplish all of this in practice is unclear. What *is* clear is that the status quo is unacceptable.

This Report proceeds in four Parts. In Part I, we survey the policing tech landscape and examine why policymakers largely have failed to regulate police use of emerging technologies. We then describe the result: a race to the ethical bottom in which any intrusive technological tool that can be dreamt up is sold to policing agencies and put into effect with little or nothing in the way of controls. In Part II, we propose certification for policing technologies as part of the solution. As we explain, certification might facilitate the enactment of hard law by addressing key challenges facing policymakers, including the lack of objective information and expertise about policing technologies. Moreover, certification could impose substantive ethical standards and create an incentive for vendors to compete along ethical lines. In Part III, we discuss a set of critical design choices for a policing certification scheme—how, for example, ought a certifier measure a product’s “benefits?” How could it account for the myriad ways that products might be used (or misused) in the real world? Finally, Part IV addresses some key challenges facing certification, including democratic legitimacy concerns, problems of compliance and enforcement, and the possibility that certification could function as a permission structure for agencies to acquire new technologies.

15. We recently applied a similar tool, an “audit,” to the latest iteration of Baltimore’s aerial surveillance program and found it severely wanting. See FRIEDMAN ET AL., *supra* note 7, at 3. Those planes no longer fly over Baltimore. See Mitchell Clark, *Baltimore’s Spy Planes Will Fly No More*, THE VERGE (Feb. 5, 2021), <https://www.theverge.com/2021/2/5/22267303/baltimore-maryland-shut-down-spy-plane-surveillance-program-vote>.

II. DEFINING THE PROBLEM

The use of emerging technologies by policing agencies is beset by two key problems.

The first problem can be thought of as structural: policymakers largely have abdicated their responsibility to regulate policing tech. A foundational principle of American governance is that executive agencies must be democratically accountable. That is, there must be rules—rules set ahead of time, with an opportunity for input from the public. If policing operated like other areas of government, legislators would put in place a means of assessing whether there is a policy framework under which use of a new technology can produce public safety benefits, while minimizing civil rights and civil liberties harms. Unfortunately, this sort of democratic accountability around policing technologies is all too rare.

The second problem is a consequence of the first: in the absence of regulation, tech vendors are enmeshed in a race to the ethical bottom, innovating new and ever more intrusive ways to track and surveil the citizenry. These technologies are marketed aggressively to policing agencies—often with completely unfounded claims about their public safety benefits. And agencies use these tools with little in the way of controls that mitigate their civil rights and civil liberties impact.

This Section proceeds in three parts. First, we survey the policing tech landscape—one defined by explosive change and a yawning information gap. Second, we explore the reasons why policymakers largely have failed to regulate police use of emerging technologies. And third, we describe the predictable result: a race to the bottom in which any intrusive technological tool that can be dreamt up is sold to policing agencies and put into effect with little or nothing in the way of controls.

A. THE POLICING TECH LANDSCAPE: WIDESPREAD USE, UNQUANTIFIED BENEFITS AND HARMS

Although early police in the United States had not much more than a nightstick at their disposal, many of today's agencies have a raft of sophisticated digital tools to choose from, ranging from aerial surveillance drones to biometric identification technologies to automated license plate readers, and much more.¹⁶ And they are putting these tools to use. Take, for

16. See generally Mathieu Deflem, *History of Technology in Policing*, in ENCYCLOPEDIA OF CRIMINOLOGY AND CRIMINAL JUSTICE 2269 (Gerben Bruinsma & David Weisburd eds., 2014).

example, face recognition technology (FRT). In 2016, a landmark report on law enforcement use of FRT estimated that one in four agencies have access to this tool, with over 117 million American adults already in face recognition databases.¹⁷ More recent investigative reporting revealed that nearly 7,000 public agency officials used FRT provided by Clearview AI—a company that scrapes billions of images from the internet without permission—often without any agency oversight.¹⁸

For many policing agencies, especially larger ones, face recognition is just the tip of the iceberg. In New York, the public learned for the first time (thanks to recently passed transparency legislation) that the New York Police Department (NYPD) has over 30 discrete surveillance tools at its disposal.¹⁹ The NYPD is by no means the only agency with access to these high-powered devices. Investigative reporting has revealed widespread use of surveillance technologies like cell-site simulators, mobile device forensic tools (MDFT), and automated license-plate readers (ALPRs) by thousands of agencies across the country. Over 2,000 agencies have purchased MDFTs, tools that enable police to download and programmatically search all data contained on a cellphone—from emails to texts to location data and more.²⁰ As far back as 2012, 71% of police departments were using ALPRs, resulting in scans of hundreds of millions of license plates.²¹ A 2020 California state auditor report

17. See GEORGETOWN L. CTR. ON PRIV. & TECH., *THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA* 1 (2016), <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf>.

18. See Ryan Mac, Carolina Haskins, Brianna Sacks & Logan McDonald, *Surveillance Nation*, BUZZFEED NEWS, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition> (Apr. 9, 2021) [hereinafter Mac, *Surveillance Nation*].

19. See *Policies*, N.Y. POLICE DEP'T, <https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page> (last visited Mar. 31, 2022) (disclosing use and impact policies for over 30 surveillance technologies pursuant to the Public Oversight of Surveillance Technology Act, N.Y. CITY ADMIN. CODE § 14-188 (2020)); see also Ali Watkins, *How the N.Y.P.D Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. TIMES (Oct. 13, 2021), <https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html> (reporting that the scope of N.Y.P.D's "surveillance dragnet" became clear "[o]nly recently" due to passage of transparency-forcing legislation).

20. LOGAN KOEPKE, EMMA WEIL, URMILA JANARDAN, TINUOLA DADA & HARLAN YU, UPTURN, *MASS EXTRACTION: THE WIDESPREAD POWER OF U.S. LAW ENFORCEMENT TO SEARCH MOBILE PHONES* 4 (2020), <https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf>.

21. See AXON AI & POLICING TECH. ETHICS BD., *2D REPORT: AUTOMATED LICENSE PLATE READERS* 13 (2019), <https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/>

revealed that the Los Angeles Police Department alone had stored more than 320 million license plate scans—99.9% of which were stored despite *not* generating a hot list match.²² Initially introduced in the 1990s to locate stolen vehicles, agencies now use ALPRs to conduct automated checks for unpaid parking tickets or inclusion in a gang database.²³ And thanks to improved data storage capabilities, these scans, which include time and location information, typically are stored and retained, creating massive databases that can track people’s movements over time.²⁴

In short, law enforcement use of technologies with super-charged abilities to collect information and conduct surveillance is widespread.

The widespread use of surveillance technologies by law enforcement might not be so concerning if the evidence were unequivocal that these tools made us safer and if communities were making informed choices to authorize the use of these tools, well aware of the potential harms. Unfortunately, neither of these things is true. Agencies deploy surveillance technologies with little information about effectiveness.²⁵ Undoubtedly some technologies have some benefits (while some may have little benefit at all), but there is almost no study of this issue. And what there is suggests the public safety benefits of even prominent technologies may be negligible.²⁶ The public and lawmakers often

Axon_Ethics_Report_2_v2.pdf; Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. (Sept. 10, 2020), <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>.

22. CAL. STATE AUDITOR, AUTOMATED LICENSE PLATE READERS 1 (2020), <http://auditor.ca.gov/pdfs/reports/2019-118.pdf>.

23. See AXON AI & POLICING TECH. ETHICS BD., *supra* note 21, at 13 (tracing the origins of police use of license plate readers to combatting auto theft); Díaz & Levinson-Waldman, *supra* note 21 (reporting on police use of license plate readers to create databases that can search for individuals with unpaid parking tickets or purported gang affiliations).

24. AXON AI & POLICING TECH. ETHICS BD., *supra* note 21, at 24–25.

25. See Cynthia Lum, Christopher S. Kroper & James Willis, *Understanding the Limits of Technology’s Impact on Police Effectiveness*, 20 POLICE Q. 135, 136–37 (2016); see also KEVIB STROM, OFF. OF JUST. PROGRAMS, RESEARCH ON THE IMPACT OF TECHNOLOGY ON POLICING STRATEGY IN THE 21ST CENTURY, FINAL REPORT (2016), <https://www.ojp.gov/pdffiles1/nij/grants/251140.pdf> (citing a body of research finding that agencies “select, implement, and integrate technology independent of existing empirical evidence or support for how these systems affect departmental operations, strategic decisions, or crime outcomes”).

26. STROM, *supra* note 25, at 4-4 (observing that “despite dramatic advances in DNA technology and computer databases for handling forensic data, clearance rates for violent and property crime have remained relatively stable since the mid-1990s” and citing studies); see also Lum et al., *supra* note 25 (generally reviewing the issue).

lack basic information and data about agency acquisition and use, rendering farcical any notion of democratic oversight.²⁷

The harms that flow from use of these technologies likewise are difficult to quantify, but there is still compelling evidence of their impact. Scholars have explained at length the theoretical and normative bases for how state surveillance chills the exercise of civil liberties and grants undue power to state actors.²⁸ Empirical research and historical experience has borne out these effects.²⁹ Worse still, these civil libertarian harms do not fall evenly upon all members of society. First, throughout American history surveillance technologies in the hands of the state have been deployed disproportionately on marginalized communities, especially Black communities.³⁰ From the FBI's COINTELPRO program to current day examples of police monitoring of Black Lives Matter activists, there is a persistent inclination of law enforcement to surveil minority communities.³¹ Second, these tools repeatedly have been used on those seeking social change by exercising First Amendment liberties.³²

27. See Mac, *Surveillance Nation*, *supra* note 18; Mihir Zaveri, N.Y.P.D. *Robot Dog's Run Is Cut Short After Fierce Backlash*, N.Y. TIMES (Apr. 28, 2021), <https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html>; Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. (forthcoming 2022).

28. E.g., Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935; see also Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications (explaining a taxonomy of privacy harms).

29. Richards, *supra* note 28, at 1948 (“Our cultural intuitions about the [chilling] effects of surveillance are supported by . . . the empirical work of scholars in the interdisciplinary field of surveillance studies.”); Karen Gullo, *Surveillance Chills Speech—As New Studies Show—And Free Association Suffers*, ELEC. FRONTIER FOUND. (May 19, 2016), <https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association> (citing studies showing that government surveillance discourages speech and access to information on the Internet).

30. See generally SIMONE BROWN, DARK MATTERS: ON SURVEILLANCE OF BLACKNESS (2015); BARTON GELLMAN & SAM ADLER-BELL, THE CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE (2017), <https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf>.

31. MUDASSAR TOPPA & PRINCESS MASILUNGAN, STRUGGLE FOR POWER: THE ONGOING PERSECUTION OF BLACK MOVEMENT BY THE U.S. GOVERNMENT 1 (2021), <https://m4bl.org/wp-content/uploads/2021/08/Struggle-For-Power-The-Ongoing-Persecution-of-Black-Movement-by-the-U.S.-Government.pdf>. COINTELPRO was a covert federal surveillance program run by the FBI during the Cold War that targeted civil rights leaders and other political dissidents. See *More About FBI Spying*, AM. C.L. UNION, <https://www.aclu.org/other/more-about-fbi-spying> (last visited Mar. 31, 2022).

32. See e.g., Joanne Cavanaugh Simpson & Marc Freeman, *South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors*, SUN SENTINEL (June 26, 2021), <https://>

There already are too many examples of the newer technologies—from face recognition to social media monitoring to aerial drones—being used to surveil lawful protestors speaking up against racial injustice.³³

More concretely, the harms that flow from these technologies also include false arrests and other wrongful enforcement actions. For example, law enforcement use of face recognition has led to three publicly known false arrests, all of Black men. Erroneous ALPR reads have led to faultless drivers being stopped and subjected to search and arrest. In Colorado, police detained, handcuffed and arrested a Black mother and her children after an ALPR scan incorrectly identified her car as stolen.³⁴ The chair of the Oakland Privacy Advisory Commission was stopped and held at gunpoint after a spurious ALPR scan.³⁵ These are but a few examples, but they are representative of the risks inherent in police use of these technologies. Yet, our ability to catalogue and quantify the scope and extent of technology-induced or enabled wrongful enforcement actions precisely is limited by the lack of basic information and transparency around law enforcement use of these tools.³⁶

In sum, the policing tech landscape can be defined by a massive information gap, which leaves us all in the dark regarding the benefits and harms and hinders democratic oversight—which we turn to next.

www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sl15uuaqfbeba32rndlv3xwxi-htmlstory.html; Sam Biddle, *U.S. Marshals Used Drones to Spy on Black Lives Matter Protests in Washington D.C.*, THE INTERCEPT (Apr. 22, 2021), <https://theintercept.com/2021/04/22/drones-black-lives-matter-protests-marshals/>.

33. See Allie Funk, *How Domestic Spying Tools Undermine Racial Justice Protests*, FREEDOM HOUSE (June 22, 2020), <https://freedomhouse.org/article/how-domestic-spying-tools-undermine-racial-justice-protests>.

34. Jessica Porter, *Aurora Police Detain Black Family After Mistaking Their Vehicle as Stolen*, THE DENVER CHANNEL (Aug. 3, 2020), <https://www.thedenverchannel.com/news/local-news/aurora-police-detain-black-family-after-mistaking-their-vehicle-as-stolen>.

35. See Lisa Fernandez, *Privacy Advocate Sues CoCo Sheriff's Deputies After License Plate Readers Target His Car Stolen*, KTVU FOX 2 (Feb. 19, 2019), <https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen>.

36. See Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> (reporting Clare Garvie's comment in response to false arrest from FRT identification: "I strongly suspect this is not the first case to misidentify someone to arrest them for a crime they didn't commit. This is just the first time we know about it.").

B. THE ACCOUNTABILITY GAP

As a democratic society, we typically turn to legislation, regulation, and/or judicial review to address the types of harmful effects described above.³⁷ All of these measures are examples of “hard law” solutions, i.e., governance mechanisms with the force of law.³⁸ Yet, these measures have been few and far between. And hard law—standing alone—inevitably falls short in addressing the challenges presented by emerging police technologies.

1. *The current hard law landscape*

This Section provides a brief overview of current hard law oversight of policing technology and its limitations.

a) The limited constraints of constitutional judicial review

The Fourth Amendment—implemented by judges—is the primary constitutional restraint on police power, but under existing doctrine, remarkably few of the emerging police technologies fall within its ambit.³⁹ Under current law, individual conduct that takes place in public, or information given to third parties, is unprotected.⁴⁰ Even when the Fourth Amendment applies, the traditional tools of warrants and probable cause are of little help when mass data collection (such as is the case with automated license plate readers) is occurring. Similarly, when it comes to racial justice concerns, current equal protection jurisprudence fails to offer meaningful recourse, as it has been interpreted to prohibit only intentional discrimination by government agencies and officers; policies and practices that have a

37. See, e.g., Gary Marchant, Lucille Tournas & Carlos Ignacio Gutierrez, *Governing Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence*, 61 JURIMETRICS J. 1, 4 (2020).

38. See *id.* at 4, 7 (comparing hard law solutions to soft law solutions).

39. See Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 838 (2004) (“Most existing Fourth Amendment rules in new technologies are based heavily on property law concepts, and as a result offer only relatively modest privacy protection in new technologies. . . . The key implication . . . is that we should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies.”); see also Andrew Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1107–08 (2021) (“[D]esigned to restrain police power and enacted to limit governmental overreach . . . current [Fourth Amendment] doctrine and constitutional theory offer little privacy protection and less practical security than one might expect.”).

40. BARRY FRIEDMAN, HOOVER INST., PRIVATE DATA/PUBLIC REGULATION 6 (2021), <https://www.hoover.org/research/private-datapublic-regulation>.

disparate racial impact largely get a free pass in the courts.⁴¹ As Rachel Harmon summarizes it, “the public policy problems presented by the use of police power necessarily extend beyond constitutional law and the courts.”⁴²

b) Current legislative approaches: few and far between

The poor fit of constitutional review is especially concerning because it has served as our primary method of addressing policing, with legislation and administrative regulation historically taking a back seat.⁴³ At the federal level, legislation addressing policing is sparse. There is some regulation of police use of technology, such as the Electronic Communications Privacy Act, which includes provisions regulating government use of wiretaps.⁴⁴ There are also some federal laws that may regulate federal law enforcement’s collection and storage of personal data from biometric tools, such as the Privacy Act of 1974 and the E-Government Act of 2002.⁴⁵ In general, though, as many scholars have observed, “federal legislation [regulating policing] is limited in scope and often badly out of date.”⁴⁶

Regarding the tech companies, Congress “so far has done next to nothing to regulate them.”⁴⁷ There is some indication that the tide may be turning on

41. See e.g., Alexis Karteron, *Congress Can’t Do Much About Fixing Local Police—But it Can Tie Strings to Federal Grants*, THE CONVERSATION (June 1, 2021), <https://theconversation.com/congress-cant-do-much-about-fixing-local-police-but-it-can-tie-strings-to-federal-grants-159881>.

42. Rachel Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 763 (2012); see also Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 NYU L. REV. 1827, 1865 (2015) (“[F]or the most part, we look to the courts to tell police when they have overstepped their bounds. The difficulty is that . . . constitutional judicial review is completely inadequate for this task.”).

43. For an exposition of why policing agency regulation historically has been the province of judicial review, see generally Friedman & Ponomarenko, *supra* note 42.

⁴⁴18 U.S.C. §§ 2510–2522; see also CHARLES DOYLE, CONG. RSCH. SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 24–28 (2012), <https://crsreports.congress.gov/product/pdf/R/R41733/9> (discussing applicability of ECPA provisions to government actors).

45. See KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT 8–9 (2020), <https://crsreports.congress.gov/product/pdf/R/R46541> (discussing applicability of federal privacy legislation to face recognition technology).

46. Maria Ponomarenko, *Rethinking Police Rulemaking*, 114 N.W. L. REV. 1, 60 (2019) [hereinafter Ponomarenko, *Rethinking Police Rulemaking*].

47. Ed. Board, *Do Your Job and Regulate Tech, Congress—or States will Try to Do it for You*, WASH. POST (Feb. 19, 2021), https://www.washingtonpost.com/opinions/maryland-digital-ads-tax-regulate-tech/2021/02/19/368ab52c-721c-11eb-93be-c10813e358a2_story.html; Shira Ovide, *What Congress Wants from Big Tech*, N.Y. TIMES (June 24, 2021), <https://>

this account. For example, the Federal Trade Commission recently warned it would use its statutory grants of authority to regulate certain tech vendor practices, action which, if taken, could implicate some policing technologies.⁴⁸ Still, as it stands, unlike with cosmetics, medical devices, or products with environmental implications, there is no comprehensive federal legislative framework establishing rules and guidelines for policing technologies.

Although there is more legislative activity addressing policing technologies at the state and local levels, it still represents the exception more than the rule.⁴⁹ And it tends to focus on a single technology at a time. For example, 16 states have statutes addressing the use of ALPRs; fewer than a dozen states have passed legislation addressing law enforcement use of FRT.⁵⁰ This tech-by-tech statutory approach means “legislatures are delivering piecemeal rather than systemic, legislation” that is “tailored to the technology [du jour] rather than to the harm.”⁵¹ With new technology perpetually coming to market, a tech-by-tech statutory approach means legislators constantly are playing catch-up.

There also are some local jurisdictions that have passed information-forcing legislation, based on a model statute developed by the ACLU, Community Control Over Police Surveillance (CCOPS), that requires disclosure around law enforcement use of surveillance technologies. Despite its broader scope, this type of information-forcing legislation has struggled to make an impact. Since the ACLU launched its CCOPS legislative campaign in 2016, only 22 municipalities across the country have adopted this law. And several of these jurisdictions have seen agencies completely fail to comply with

www.nytimes.com/2021/06/24/technology/congress-big-tech.html (discussing recently proposed legislation to reign in big tech).

48. Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (Apr. 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

49. Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 61 (“In policing . . . states do quite a bit more.”).

50. *E.g.*, AMBER WIDGERY, NAT'L CONF. STATE LEGISLATORS, LAW ENFORCEMENT USE OF TECHNOLOGY 16–17 (2021), <https://www.nmlegis.gov/handouts/CCJ%20072621%20Item%206%20Widgery%20Tech%20Slides%20final.pdf>. There also are a handful of states that regulate the collection of biometric information by private companies, protections which could apply to tech vendors that sell biometric tools to law enforcement. *See* Natalie Prescott, *The Anatomy of Biometrics Law: What U.S. Companies Need to Know in 2020*, THE NAT'L L. REV. (Jan. 15, 2020), <https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020>.

51. Maily Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 SANTA CLARA HIGH TECH. L.J. 481, 544 (2020).

the statutory requirements.⁵² Others have seen agencies issue generic disclosures devoid of any meaningful information about use or impact. For example, in New York City, where the City Council passed a CCOPS-inspired statute, a coalition of 14 civil rights organizations and advocates, including the local chapter of the ACLU, found that the NYPD’s “boilerplate” responses were “plainly insufficient” and did not “reflect a good faith effort to comply” with statutory requirements.⁵³ In Oakland, the police department’s failure to comply with CCOPS legislation has led to a lawsuit from the chair of the Privacy Advisory Commission (PAC), the public body charged with oversight, who concluded that “the model is failing to work in Oakland and the other jurisdictions.”⁵⁴

c) Administrative body regulation: exceptions rather than rule

A handful of cities have turned to administrative agency solutions for oversight of policing technology acquisition and use—an approach that some policing scholars have touted as a particularly apt governance solution.⁵⁵ For example, Oakland’s PAC is an administrative body that, in conjunction with the City Council, oversees acquisition and use of any surveillance technologies used by law enforcement.⁵⁶ In addition, a number of major cities, including

52. *Community Control over Police Surveillance*, ACLU, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance> (last visited Jan. 22, 2022); see, e.g., Ali Watkins, *How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. TIMES (Sept. 8, 2021) <https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html> (noting NYPD’s reluctance to fully comply with transparency requirements in POST Act, a watered-down version of CCOPS).

53. Letter from the N.Y. C.L. Union to Dermot Shea, Comm’r, N.Y.C. Police Dep’t (Feb. 24, 2021), https://www.nyclu.org/sites/default/files/field_documents/nyclu_letter_on_post_act_draft_policies_0.pdf; Letter from Civ. Soc’y to Dermot Shea, Comm’r, N.Y.C. Police Dep’t, & Margaret Garnett, Comm’r of the Dep’t of Investigation, Regarding the Public Oversight of Surveillance Technology Act (Feb. 24, 2021), <https://static1.squarespace.com/static/5c1bfc7ee175995a4ceb638/t/6036a7b9952aac14fd3df39d/1614194617915/POST+Act+Joint+Submission+%2802-24-21%29.pdf>.

54. Brian Hofer, *Why You Should Care About Our Lawsuit Against the City of Oakland*, SECURE JUST. (Sept. 2, 2021), <https://secure-justice.org/blog/why-should-you-care-about-our-lawsuit-against-the-city-of-oakland>.

55. See Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 1, 45–59 (arguing that we should consider creating “regulatory intermediaries” or permanent administrative bodies—such as inspectors generals or police commissions—that can stand in for the public to regulate the police); see also Fidler, *supra* note 51, at 481–82 (proposing that rather than legislate on these issues, city councils or a local appointed commission should be empowered to regulate the acquisition and deployment of police surveillance technologies).

56. Fidler, *supra* note 51, at 548–49; *Privacy Advisory Commission*, CITY OF OAKLAND, <https://www.oaklandca.gov/boards-commissions/privacy-advisory-board> (last visited Jan. 22, 2022).

Detroit, Los Angeles, San Francisco, and Chicago, have citizen-run police commissions that govern their police departments.⁵⁷ Regarding policing technologies specifically, several leading computer scientists recently have called for a new federal office—modeled on the Food and Drug Administration (FDA)—to regulate the use of face recognition technology by private and public actors, though nothing like this currently exists.⁵⁸ Still, despite these few promising examples and proposals, administrative agency bodies remain the exception not the rule for police technology oversight. And generalist commissions have done little to address technology issues.

2. *Obstacles facing hard law regulation of policing technology*

There are a set of obstacles that explain why the current regulatory landscape is sparse and inadequate. These obstacles set the stage for turning to certification as a possible partial solution:

a) Pacing Problem

Technological development today is happening “at an unprecedented pace,” which makes it “harder than ever to govern using traditional legal and regulatory means”—a phenomenon commonly referred to as the “pacing problem.”⁵⁹ Policing technology development is no exception. For example, in its evaluations of face recognition algorithms, the National Institute of Standards and Technology (NIST) reported “massive gains in accuracy” in the last five years, which “far exceeded” the improvements made in the preceding period.⁶⁰ Because government regulation is an inherently slow and bureaucratic process, it increasingly is difficult for it to keep up with these rapid

57. Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 47; Annie Sweeney, *Mayor Names Leader of New Civilian Commission Overseeing Chicago Police Department*, CHI. TRIB. (Jan. 10, 2022), <https://www.chicagotribune.com/news/criminal-justice/ct-civilian-police-oversight-head-20220110-so2f5xbra5ethppinotkjjfmhe-story.html>.

58. ERIK LEARNED-MILLER, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & JOY BUOLAMWINI, *FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE* (2020), https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRT'sFederalOfficeMay2020.pdf.

59. See Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 59 (2018); see also Adam Thierer, *The Pacing Problem, the Collingridge Dilemma & Technological Determinism*, TECH. LIBERATION FRONT (Aug. 16, 2018); Gary Marchant et al., *Addressing the Pacing Problem in THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT* 199 (2011).

60. Charles Romine, *Facial Recognition Technology (FRT)*, NAT'L INST. OF STANDARDS & TECH. (“NIST”) (Feb. 6, 2020), <https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0>.

developments in policing technologies.⁶¹ Perhaps worse, this rapid pace of development could mean that even if regulators could hurry to act, regulation “will likely be obsolete by the time the ink dries on the enactment.”⁶²

b) An Information Gap

This rapid pace of development and the inherent newness and uncertainty surrounding emerging technologies makes it difficult for policymakers to have the information required to support traditional regulation.⁶³ Put simply, new products enter the market ahead of scientific certainty about their benefits and harms, making it difficult, if not impossible, for regulators to have sufficient information with which to conduct an evaluation. Nor does there seem to be much effort to assess benefits and harms once these technologies are in use. With policing technologies, there also tend to be additional layers of obscurity around these products’ mere existence—often in the name of security—that inhibit legislative and regulatory oversight. For example, after the NYPD deployed a robotic surveillance dog without city council approval, councilmembers had to issue subpoenas to obtain basic details about its procurement.⁶⁴ A recent report issued by the U.S. Government Accountability Office (GAO) found that out of 14 federal law enforcement agencies that reported using external FRT systems, 13 had *no idea* which systems their personnel were using.⁶⁵ One agency initially informed the GAO that it did not use any external FRT systems but was forced to correct this representation after an internal poll showed that its employees had conducted over 1,000 face

61. See Gary E. Marchant, Douglas J. Sylvester & Kenneth W. Abbott, *A New Soft Law Approach to Nanotechnology Oversight: A Voluntary Product Certification Scheme*, 28 UCLA J. ENV'T L. & POL'Y 123, 130 (2010); Gary Marchant & Wendell Wallach, *Toward the Agile and Comprehensive International Governance of AI and Robotics*, 107 POINT OF VIEW 505, 505 (2019), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8662741> (“Rapidly emerging technologies . . . are advancing so quickly that in many sectors, traditional regulation cannot keep up, giving the cumbersome procedural and bureaucratic procedures and safeguards that modern legislative and rulemaking processes require.”); see also Hagemann et al., *supra* note 59, at 58–59, 61 (discussing “the accelerating pace of ‘the pacing problem’” and arguing that “[m]odern technological innovation is occurring at an unprecedented pace, making it harder than ever to govern using traditional legal and regulatory mechanisms”).

62. Marchant & Wallach, *supra* note 61.

63. Marchant et al., *supra* note 61, at 130.

64. See Zaveri, *supra* note 27.

65. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-105309, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD HAVE BETTER AWARENESS OF SYSTEMS USED BY EMPLOYEES 10 (2021), <https://www.gao.gov/assets/gao-21-105309.pdf>.

recognition searches on external systems.⁶⁶ Without basic information about which products agencies are even using, neither legislators nor the public can begin to evaluate these tools.

c) An Expertise Gap

Even when there is awareness and knowledge about law enforcement use of these technologies, policymakers often lack the expertise needed to adequately evaluate these increasingly complex tools.⁶⁷ In particular, new policing tools that incorporate machine learning (ML) technology can require advanced degrees in computer and data sciences to analyze their functions and limitations.⁶⁸ Legislators face an ever-steeper learning curve in the face of these new developments. Yet effective legislation and regulation requires a full understanding of how these technologies work and interact with each other, their capabilities, their flaws, and their impact on people. In our current system, it is difficult if not impossible for legislators and regulators to acquire this level of understanding.

d) A Public Choice Problem

In the absence of digestible information about the risks these technologies pose, anti-regulatory pressures from interest groups like police unions and other law enforcement organizations dominate.⁶⁹ Even in the wake of widespread calls for police reform, being labeled “soft on crime” remains a political death knell.⁷⁰ Consider the collapse of bipartisan negotiations around federal police reform legislation because of an inability to reach consensus

66. *Id.* at 11.

67. Timothy Lytton, *Competitive Third-Party Regulation: How Private Certification Can Overcome Constraints That Frustrate Government Regulation*, 15 THEORETICAL INQUIRIES L. 539, 543 (2013) (explaining how “limited expertise” can frustrate government efforts to regulate); Hagemann et al., *supra* note 59, at 69 (discussing the “knowledge problem” regulators face when it comes to emerging technologies and the lack of regulatory expertise); Fidler, *supra* note 51, at 530 (“Neither judges nor legislators nor municipal officials will be experts on investigative technology. . . . Administrative oversight does not solve this [expertise] problem.”); *see generally* Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46.

68. *See* Sebastian Klovig Skelton, *UK Regulators Lack The Skills and Expertise to Cope with Increasing Use of Algorithms*, COMPUTERWEEKLY.COM (Oct. 15, 2020), <https://www.computerweekly.com/news/252490597/UK-regulators-lack-the-skills-and-expertise-to-cope-with-increasing-use-of-algorithms>.

69. Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 62 (“Police unions and other law enforcement organizations are a powerful force in state-level politics.”).

70. Friedman & Ponomarenko, *supra* note 42, at 1863–64 (discussing legislative inaction on policing and observing that “[t]here are few labels in American politics more damning than ‘soft on crime.’ For the most part, then, legislatures are content to leave well enough alone.”).

around qualified immunity, a deal breaker for police unions.⁷¹ As public choice theory would predict, legislators are reticent to step into the fray of contentious issues for fear of offending powerful interest groups or large segments of their voters and thereby hurting their chances of reelection.⁷²

Policymakers also face anti-legislative pressures from industry, particularly in light of the competitive national and international marketplaces. As in the tech industry writ large, policing technology vendors employ powerful lobbying groups across Washington and statehouses. Many vendors operate across state or national borders, creating downward pressure on both local and national governments to impose restrictive regulations that could impede their competitiveness in the broader marketplace.⁷³

e) Federalist Fragmentation

Pace aside, state and local hard law solutions for policing technologies also present problems of fragmentation. By and large, these technology products are not designed for a particular agency or deployed in a single jurisdiction. They mostly are off-the-shelf tools that raise similar concerns wherever they are deployed. Relying on local legislation or regulation as a solution means expecting each jurisdiction to develop its own evaluative matrix for these complex tools. Take the example of a face recognition algorithm that research has shown can produce racially biased results. How is an ordinary lay entity expected to vet this claim? By reviewing the black box of machine learning code to see if a particular system exhibits this bias? Such a localized analysis

71. Jacob Pramuk, *Police Reform Talks Fall Apart after Months of Bipartisan Negotiations in Congress*, CNBC (Sept. 22, 2021), <https://www.cnbc.com/2021/09/22/police-reform-booker-bass-scott-negotiations-fall-apart.html>; see also Fidler, *supra* note 51, at 542–43 (“[C]ongressional interest has waned for [many policing] technologies. . . . Little federal Congressional action on related [issues] has happened since the early 2000s.”).

72. See Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice*, 44 SYRACUSE L. REV. 1079, 1086–92 (1993) (detailing the relationship between voters, legislators, and criminal procedure decisions); Ronald Wright, *Parity of Resources for Defense Counsel and the Reach of Public Choice Theory*, 90 IOWA L. REV. 219, 257–58 (2004) (discussing legislatures’ willingness to approve and fund, rather than restrict, police activity because benefits are generalized while surveillance harms disproportionately affect already marginalized groups); cf. Rachel Barkow, *Federalism and the Politics of Sentencing*, 105 COLUM. L. REV. 1276, 1278–83 (2005) (describing the public choice problem in sentencing law).

73. Hagemann et al., *supra* note 59, at 71–74; see also GARY MARCHANT, AI PULSE, SOFT LAW GOVERNANCE OF ARTIFICIAL INTELLIGENCE 3 (2019), <https://aipulse.org/soft-law-governance-of-artificial-intelligence/?pdf=132> (discussing regulation of emerging AI technologies and concluding that “national governments are reluctant to impede innovation in an emerging technology by preemptory regulation in an era of intense international competition”).

would be inefficient, unrealistic, and risk the creation of inconsistent and conflicting conclusions across jurisdictions.⁷⁴ Although federal legislation might avoid this fragmentation problem, it still would have to wrestle with federalism constraints when it comes to oversight of local policing.⁷⁵

C. THE RESULTANT RACE TO THE BOTTOM

In the absence of adequate legislation and regulation, market forces hold sway, creating a race to the bottom in which any intrusive technological tool that can be dreamt up is sold to policing agencies and put into effect with little or nothing in the way of controls. Policing agencies, which consider it their mission to keep the public safe, seek and purchase products that they are told by vendors promise the greatest security benefits. Producers of these technologies innovate to meet this demand, focusing on tools that assist agencies in gathering information about and from the public, while paying little attention to ethical implications.⁷⁶ Although the public and elected officials have an interest in protecting civil rights and liberties, their ability to surface their demand for these criteria is stymied by the information, expertise, and public choice problems described above.⁷⁷ Simply put, when it comes to policing technologies, we have a race to the ethical bottom.

74. See, e.g., Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 45 (discussing local administrative regulatory bodies for police oversight, with over 18,000 agencies, “these sorts of regulatory structures may not be a viable solution to the problems of policing writ large”).

75. Fidler, *supra* note 51, at 541–42 (“[P]artway is the furthest we’d get with a top-down federal approach.”).

76. See David Priest, *Ring’s police problem never went away. Here’s what you still need to know*, CNET (Sept. 27, 2021), <https://www.cnet.com/home/security/rings-police-problem-didnt-go-away-it-just-got-more-transparent/>; April Glaser, *How to Not Build a Panopticon*, SLATE (July 19, 2019), <https://slate.com/technology/2019/07/amazon-rekognition-surveillance-panopticon.html> (reporting on the successful expansion of Amazon’s Ring product without consideration for its civil liberties concerns); Priyanka Boghani, *Amazon Exec Defends Recognition Sales to Law Enforcement, Says Would Sell to Foreign Governments*, PBS FRONTLINE (Feb. 8, 2020), <https://www.pbs.org/wgbh/frontline/article/amazon-aws-ceo-andy-jassy-defends-facial-recognition-sales-law-enforcement-says-would-sell-to-foreign-governments> (describing Amazon’s push to sell facial recognition technology to law enforcement despite concerns raised by civil rights groups); see also Elizabeth Joh, *The Undue Influence of Surveillance Companies on Policing*, 92 N.Y.U. L. REV. 19, 20–21 (2017) (observing that despite surveillance technology vendors’ significant influence over police, vendors largely are not publicly accountable for their products’ impacts on civil liberties).

77. See Kira Matus, *Standardization, Certification, and Labeling: A Background Paper for the Roundtable on Sustainability Workshop January 19–21, 2009*, in CERTIFIABLY SUSTAINABLE? THE ROLE OF THIRD-PARTY CERTIFICATION SYSTEMS: REPORT OF A WORKSHOP 79, 83–84 (2010), <https://www.nap.edu/read/12805/chapter/12> (discussing how certification can be a

But the fact that the hard law governance landscape currently is insufficient is neither surprising nor cause to lose hope for effective oversight of policing technologies. Many of the regulatory challenges described above are common across sectors dealing with emerging technologies from the financial industry to biomedicine.⁷⁸ Rather, it is reason to explore whether there are other approaches that may help remove some of the obstacles facing legislative and regulatory approaches or fill in the regulatory void, at least in part. As Gary Marchant has explained, emerging technology governance is a “wicked problem” for which “there will not be a single, effective solution . . . [r]ather, the best strategy will be to integrate a number of imperfect tools, recognizing and trying to compensate for their particular flaws.”⁷⁹

In the remainder of this Report, we explore whether a “soft law” tool, namely a product certification system, might have a role to play in solving the “wicked problem” of emerging policing technology governance.

III. PRODUCT CERTIFICATION AS PART OF THE SOLUTION?

A. WHAT WE’RE EXPLORING

So far, we’ve seen two general problems: there is not enough hard law to regulate policing technologies because of a set of factors—pacing, lack of information, lack of expertise, political self-interest, and the regulatory fragmentation of our federal system; and there is a resultant race to the bottom. Here, we explore the idea of certification as a partial solution to these problems. Certification systems “attempt[] to harness market forces” to promote a particular goal or set of goals that currently are ignored or undervalued in the marketplace.⁸⁰ They are a form of “soft law”—or “program[s] that create[] substantive expectations, but which are not directly

useful regulatory solution for products with impacts that may evade typical marketplace incentives).

78. Hagemann et al., *supra* note 59, at 41; *see also* GARY MARCHANT, EMERGING TECHNOLOGIES: ETHICS, LAW, AND GOVERNANCE 1 (2017) (“One of the distinguishing features of most emerging technologies is that they present a broad range and diversity of ethical and social issues.”).

79. Gary Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 VAND. L. REV. 1861, 1862–63 (2020).

80. POOJA SETH PARIKH, ENV’L L. INST., HARNESSING CONSUMER POWER: USING CERTIFICATION SYSTEMS TO PROMOTE GOOD GOVERNANCE 1 (2003), <https://www.eli.org/sites/default/files/eli-pubs/d13-05a.pdf>; *see also* Matus, *supra* note 76, at 83–84 (explaining that certification allows consumers “to have more information regarding impacts of their consumption that would otherwise be unobservable to them”).

enforceable by government.”⁸¹ Certification systems both provide an additional level of regulation, albeit without the formal enforcement of hard law, and they can provide some of the information and expertise that is needed to break the public choice logjam and enable hard law itself.

The basic concept we have been studying is a product certification system in which producers of policing technologies would submit their products for evaluation. The evaluation would involve two functions. First, it would perform some sort of *efficacy review*. At minimum, this would entail evaluating whether/how well the product does what it purports to do. Or it could go further and conduct a more holistic assessment of whether there is clear evidence for the notion that its use would enhance public safety. Second, products would undergo an *ethical review*, which would entail assessing the product along a list of dimensions including privacy, racial justice, data protection, and the like. We explore certification design in-depth in Part III. But first, some examples.

B. COMMON CERTIFICATION EXAMPLES

Product certification is not a new concept. It currently is used in varying forms across disparate industries. Common examples include:

Table 1: Examples of Certification Schemes

B Lab Certification	B Corporations are for-profit businesses that meet certain standards of “social and environmental performance,” as certified (for a fee) by the nonprofit organization B Lab. Its certification standards assess whether the corporations create value for non-shareholding stakeholders, including their employees, community members, customers, and the environment, as determined via ~200 question “Impact Assessment.” Companies also must satisfy certain legal requirements. B Lab publishes a final Impact Report, which contains a summary of a company’s Impact Assessment scores.
USDA “Organic” Certification	The U.S. Department of Agriculture (USDA) accredits state or private agencies to certify food products or farms that adopt practices that comply with the USDA’s organic regulations. Entities submit an application (with fees) to a USDA-accredited certifier, which includes a “detailed description of the operation to be certified” and a written plan “describing the practices and substances to be used.” Certifiers review the written application, and if approved, an

⁸¹. Marchant et al., *supra* note 37, at 5.

	inspector visits the operation to verify compliance. An approved entity receives an organic certificate which allows it to sell, label, or represent its products as “organic.” The USDA website maintains a database of certified organic farms and businesses with basic information about what’s been certified.
Gem Certification	The Gemological Institute of America (GIA) issues a “Diamond Grading Report” which provides information on various diamond features, including shape, clarity, cut, and carat weight. Jewelers voluntarily submit a gem for review and receive a detailed report describing the gem across these various categories. These reports often are provided to prospective purchasers. Although the GIA reports provide categorical grades, they do not make ultimate purchasing recommendations.

C. CERTIFICATION FOR POLICING TECHNOLOGY: ABSENCE AND DEMAND

Certification entities like those just described do not exist, nor have they ever, for policing technologies. Yet there presently are some proposals and programs that would require the existence of, or indicate buy-in for, certification in the policing tech space.

The European Commission’s recently proposed Artificial Intelligence Act would require high-risk AI systems used by law enforcement, such as face recognition technology, to undergo an independent pre-market certification process to assess compliance with EU specifications. These include requirements for data governance, system transparency, human oversight, accuracy, robustness, cybersecurity, and auditability.⁸² To retain their certification, these systems also will be subject to post-market surveillance and supervision.⁸³ Thus, tech vendors looking to sell their AI systems to law enforcement in Europe soon may be subject to a certification process with ethical components.

82. Eve Gaumont, *Artificial Intelligence Act: What is the European Approach for AI?*, LAWFARE (June 4, 2021), <https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai>.

83. THEODORE CHRISTAKIS, MATHIAS BECUYWE & AI-REGULATION TEAM, FACIAL RECOGNITION IN THE DRAFT EUROPEAN AI REGULATION: FINAL REPORT ON THE HIGH-LEVEL WORKSHOP HELD ON APRIL 26, 2021 (2021), <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>.

Although there is no official U.S. government parallel to the European Commission's certification proposal, a recent report issued by the Federation of American Scientists (FAS) urges federal action to create a "Digital Surveillance Oversight Committee" (DSOC), a multi-stakeholder certification body, housed in a federal agency, that would certify current and emerging surveillance technologies used by public agencies—including local law enforcement—across ethical dimensions.⁸⁴

Several non-governmental organizations recently have piloted certification systems that would include *some* technology products used by law enforcement in their remit.⁸⁵ Most notably, in 2018, the Institute of Electric and Electronic Engineers (IEEE), the world's largest technical professional organization and a major player among standards-setting organizations, launched an "ethics certification program" for AI systems (ECPAIS) with the goal of developing a certification process that would address transparency, accountability, and reduction of algorithmic bias in AI systems.⁸⁶

Although not a certification system, NIST's ongoing series of Face Recognition Vendor Tests (FRVT) bears mentioning as well. For over a decade, NIST has conducted benchmark testing to measure face recognition systems' algorithmic accuracy.⁸⁷ These tests do not certify algorithmic compliance with a particular set of national standards nor does NIST place a "seal of approval" on any particular algorithm. But, in issuing public reports ripe with vendor-specific performance data and maintaining a dynamic "leaderboard" ranking algorithm performance on its website, its evaluations and rankings have become powerful motivators for industry improvement as evidenced by vendors' frequent citation to their NIST standings in press and

84. ISHAN SHARMA, FED'N OF AM. SCIENTISTS, A MORE RESPONSIBLE DIGITAL SURVEILLANCE FUTURE 32–34 (2021), <https://uploads.fas.org/2021/02/Digital-Surveillance-Future.pdf>.

85. E.g., *The Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)*, IEEE SA, <https://standards.ieee.org/industry-connections/ecpais.html>; SEBASTIEN LOURADOUR & LOFRED MADZOU, WORLD ECONOMIC FORUM, RESPONSIBLE LIMITS ON FACIAL RECOGNITION: USE CASE: FLOW MANAGEMENT PART II (2020), https://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf. See generally *Soft Law Governance of Artificial Intelligence*, CTR. FOR L., SCI. & INNOVATION, ASU SANDRA DAY O'CONNOR COLL. OF L., <https://lsi.asulaw.org/softlaw> (last visited Jan. 27, 2022) (presenting a database of over 600 soft law programs targeting AI technologies, including certification systems).

86. IEEE SA, *supra* note 85.

87. *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 116–60 (2020) (statement of Charles H. Romine, Director of the Info. Tech. Lab'y, Nat'l Inst. Standards & Tech.).

sales materials.⁸⁸ As a result, what NIST measures can end up counting for a lot in shaping industry practice. For example, researchers have observed that NIST’s decision to evaluate demographic effects on accuracy has “ensur[ed] such concerns propagate into industry systems.”⁸⁹

The growing use of “ethics” or “advisory” boards by policing technology companies also is worth mentioning as it indicates an awareness on the part of tech companies that the status quo will not suffice. From 2019 to 2022, Axon, a major policing technology vendor, set up an AI Ethics Board made up of experts in the fields of AI, computer science, privacy, law enforcement, civil liberties, and public policy. The Board’s purpose was to guide the company “around ethical issues relating to the development and deployment of artificial intelligence (AI)-powered policing technologies.”⁹⁰ In response to the Board’s report highlighting the risks of FRT, for example, Axon agreed to not proceed with adding FRT capabilities to its body-worn cameras.⁹¹ And in a naked attempt to counter its invasive and potentially illegal practices, Clearview stood up an “independent” advisory board—staffed almost entirely with former law enforcement or national security officials—with a stated mission of ensuring

88. See, e.g., *FRVT 1: N Identification*, NAT’L INST. STANDARDS & TECH., <https://pages.nist.gov/frvt/html/frvt1N.html> (last visited Apr. 5, 2022) (linking to public report evaluating face recognition algorithms and displaying table ranking face recognition algorithm performance); *Idemia’s Facial Recognition Ranked #1 in NIST’s Latest FRVT Test*, IDEMIA (Apr. 6, 2021), <https://www.idemia.com/press-release/idemias-facial-recognition-ranked-1-nists-latest-frvt-test-2021-04-06> (citing performance on NIST testing in press release); *NEC Face Recognition Technology Ranks First in NIST Accuracy Testing*, NEC (Aug. 23, 2021), https://www.nec.com/en/press/202108/global_20210823_01.html (same); see also Samuel Dooley, Tom Goldstein & John P. Dickerson, *Robustness Disparities in Commercial Face Detection 1*, ARXIV:2108.12508 (Aug. 27, 2021), <https://arxiv.org/pdf/2108.12508.pdf> (discussing the role of NIST testing as a “guardrail that has spurred positive, though insufficient, improvements and widespread attention”).

89. Dooley et al., *supra* note 88.

90. *Axon AI Ethics Board*, POLICING PROJECT N.Y.U. SCH. OF L., <https://www.policingproject.org/axon-ethics-board> (last visited Jan. 27, 2022). In 2022, the AI Ethics Board disbanded following the resignation of nine Board members in response to Axon’s announcement that it was proceeding with development of TASER-equipped drones to be deployed in schools and other potential targets for mass shootings. See *Statement of Resigning Axon AI Ethics Board Members*, POLICING PROJECT (June 6, 2022), <https://www.policingproject.org/statement-of-resigning-axon-ai-ethics-board-members>. Axon has now announced that it is pausing work on the TASER drone project. See Rick Smith, *Axon Committed to Listening and Learning So That We Can Fulfill Our Mission to Protect Life, Together*, AXON (June 5, 2022), <https://www.axon.com/news/technology/axon-committed-to-listening-and-learning>.

91. Chaim Gartenberg, *Axon (formerly Taser) Says Facial Recognition on Police Body Cams is Unethical*, THE VERGE (June 27, 2019), www.theverge.com/2019/6/27/18761084/axon-taser-facial-recognition-ban-ethics-board-recommendation.

that its face recognition technology is “used . . . according to the highest professional standards to keep communities safe.”⁹² To date, Clearview’s Advisory Board has not taken any public action.

These proposed requirements, and emerging models, indicate that various experts and key stakeholders believe there is value to the use of some sort of certification regime to help address the governance gaps raised by policing agencies and governmental use of emerging technologies with the capacity for surveillance and information-collection.

D. CERTIFICATION AS AN ANSWER TO KEY POLICING TECHNOLOGY GOVERNANCE CHALLENGES

In theory, certification for policing technologies both could foster democratic accountability and mitigate the current race to the bottom.⁹³

1. *Supplying Information and Expertise to Foster Democratic Accountability*

A certification system for policing technologies could assist policymakers by addressing the information and expertise gaps that currently stymie effective hard law governance. By definition, certification communicates information about products.⁹⁴ Through highlighting which products policing agencies are using as well as the particular attributes and impact of these tools, certification could influence purchasing decisions by policing agencies and the jurisdictions they serve and aid regulators drafting legislation and rules. Certifiers also could require vendors to implement transparency-forcing mechanisms, such as transparency portals—online portals that could disclose information about how police use technology. In these ways, certification systems could help provide information the public and legislators currently lack—information that is essential to support traditional regulation.

92. *Clearview AI Announces Formation of Advisory Board*, BUSINESSWIRE (Aug. 28, 2021), <https://www.businesswire.com/news/home/20210818005288/en/Clearview-AI-Announces-Formation-of-Advisory-Board>.

93. See, e.g., Carlos Ignacio Gutierrez & Gary Marchant, *Soft Law 2.0: Incorporating Incentives and Implementation Mechanisms Into the Governance of Artificial Intelligence*, ORG. FOR ECON. CO-OPERATION & DEV. (July 13, 2021), <https://oecd.ai/en/wonk/soft-law-2-0> (observing that soft law mechanisms “can . . . serve as a precursor or as a complement or substitute to regulation”); Mallory Elise Flowers, Daniel C. Matisoff & Douglas S. Noonan, *In the LEED: Racing to the Top in Environmental Self-Regulation*, 29 BUS. STRATEGY & ENV’T 2842, 2843, 2852–53 (2020) (finding that a green building certification program created a “race to the top” in improving buildings’ environmental performance).

94. NAT’L RSCH. COUNCIL, CERTIFIABLY SUSTAINABLE?: THE ROLE OF THIRD-PARTY CERTIFICATION SYSTEMS: REPORT OF A WORKSHOP 19 (2010), <https://www.nap.edu/read/12805/chapter/1>.

In addition, certification systems similarly can address the expertise gaps that often prevent effective regulation. Because they have fewer barriers to employing or contracting with a broad range of subject matter experts to review and evaluate products—certification systems can draw on, they are able to acquire technical expertise that policing agencies, legislatures, and regulatory bodies cannot access as easily.⁹⁵

2. *Evading Hard Law Challenges to Curb the Race to the Bottom*

As discussed, in the absence of regulation, we are living with a technological race to the bottom—a race which certification systems could disrupt through setting substantive ethical standards. By setting standards for ethical use, a successful certification regime can construct a raised floor and create an incentive for vendors to compete along ethical lines.

Although certification should not be seen as a *replacement* for regulation, setting substantive standards through certification both can serve some helpful function in the absence of regulation and also can shore up regulation where it exists because it avoids some of the key problems facing policymakers. First, because it is a non-legislative body (whether public or private) with a distinct mission, certification will not be burdened with the public choice problems that have thrown legislative bodies into stasis. Members of this body will have no reason to fear public opinion injuring their electoral chances. And constructed properly, they would be beholden to no particular entities or interest groups. (We address the issue of industry capture in Section III.E). In addition, certification can bring salience to problems around policing tech in a way that can break the regulatory logjam.

Second, because a certification system need not comply with a panoply of bureaucratic and procedural requirements, it can better keep pace with rapid technological changes, establish standards more quickly than some regulatory bodies, and revisit issues more frequently.⁹⁶ This flexibility would enable it to keep pace with rapid technological changes.⁹⁷ For example, the entity could re-evaluate a given vendor's face recognition software whenever there is a

95. Lytton, *supra* note 67, at 564; cf. Lesley K. McAllister, *Harnessing Private Regulation*, 3 MICH. J. ENV'L & ADMIN. L. 291, 294 (2014) (noting that a “[c]ommonly cited benefit[]” of non-governmental forms of regulation is “increasing expertise”); David M. Lawrence, *Private Exercise of Governmental Power*, 61 IND. L.J. 647, 656–57 (1985) (citing the “availability of special expertise” as an advantage of delegating regulation to private actors); NAT'L RSCH. COUNCIL, *supra* note 94, at 11; Hagemann et al., *supra* note 59, at 92 (observing that “[r]egulators . . . are increasingly reliant on the expertise housed in private firms to execute best practices and standards”).

96. *Id.*

97. See, e.g., Marchant et al., *supra* note 37, at 7.

significant software update or a new use case is discovered without having to wade through more rigid agency approval processes.

Finally, a the reach of a certification entity would not be subject to can evade issues of regulatory fragmentation because it could evaluate products and producers (and perhaps uses, more on that below) at one central node, providing useful information and expertise that the many individual local entities—from policing agencies to local and state legislatures—could piggyback upon. Local jurisdictions could rely on certification results for complex algorithms, rather than having to conduct their own evaluations from scratch, an impossible task for most jurisdictions.

E. THEORIES OF CHANGE

Having laid out how certification might address the key challenges to policing tech governance, we now turn to the underlying mechanism(s) that would allow a certification entity to produce these changes, i.e., the theory (or theories) of change that would guide development.

First, certification can effect change by incentivizing tech vendors to produce more ethical and transparent products. Vendors benefit if the system helps their bottom line and/or burnishes their brand. By providing clear ethical goals toward which companies can work and a label that signals compliance, certification can help companies differentiate themselves in the marketplace and protect their reputations, thereby ending the race to the ethical bottom that many vendors are engaged in at present. After all, reputation is a “fundamental organizational asset,” and certification would serve as a tool for companies to use in promoting their social responsibility.⁹⁸ (Vendors also might value certification if it helps ward off regulation, a challenge and concern we discuss in Section IV.D.)

Second, certification can effect change by influencing policing agencies to choose products that are more ethical. Policing agencies and the jurisdictions they serve would benefit from certification because it would enable agencies to choose technologies wisely and thus use them with less concern about public backlash. Relying on emerging technology in a non-transparent way has caused a great deal of suspicion in the general public. At times, law enforcement has been denied the ability to continue using those tools altogether. For example, the Seattle Police Department had to abandon its drone program, which included two helicopter drones acquired without

98. Carlos Ignacio Gutierrez, Gary Marchant & Lucille Tournas, *Lessons for Artificial Intelligence from Historical Uses of Soft Law Governance*, 61 JURIMETRICS J. 133, 140 (2020).

democratic approval or public awareness, after facing fierce public backlash.⁹⁹ Reacting to San Francisco's ban on FRT use by law enforcement, the head of the National Police Foundation conceded that "our traditional secrecy and lack of transparency has probably come back to haunt us."¹⁰⁰ In addition, policing officials complain that they are overrun with pitches from vendors and that it is difficult to distinguish one product from another. Certification could eliminate some of this uncertainty and provide a guide to products that meet some level of ethical standards, as well as those that (at least) perform as intended. Indeed, law enforcement we spoke with repeatedly emphasized the need for a source of objective, comparative information about how these tools operate.

Third, certification can effect change by helping legislators, the media, and the public better understand and compare the ethical implications of policing technologies. The public could benefit from certification in two main ways: (1) certification could raise the salience of emerging policing technologies and thus motivate hard law regulation, and/or (2) it could create a market for products that are more protective of civil rights and liberties thus reducing harm. As Part I made clear, dysfunction in the hard law system has led to adoption of potentially harmful technologies with almost no regulation. Members of the public and the media may not know about the technologies at all, and they have no way to evaluate their purported benefits or ethical impacts. Certification could serve as a tool to disseminate the information required to produce a more transparent marketplace and prompt a functional regulatory ecosystem.

Similarly, regulators suffer at present from a host of obstacles—from lack of information and expertise to pressures not to regulate the police and thus appear soft on crime. Certification would provide needed information, vetted by experts. Certification might help with the public choice logjam as well: if some products are certified as acceptable, and others not, regulators would have a roadmap of how to proceed to regulate in a way that could attract public acceptance. Certification gives them cover of a sort. (As noted above, though, certification may deter regulation, an issue we take up Section IV.D).

The extent to which each of these theories of change are distinct or overlapping is debatable. The bottom line is that for a policing technology

99. Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 7, 2013), <https://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program>.

100. Jon Schuppe, *San Francisco's Facial Recognition Ban is Just the Beginning of a National Battle Over the Technology*, NBC NEWS, <https://www.nbcnews.com/news/us-news/san-francisco-s-facial-recognition-ban-just-beginning-national-battle-n1007186> (May 22, 2019).

certification system to work, it must be valued by some combination of the key stakeholder groups in this ecosystem: law enforcement, policymakers, the public, and tech vendors.¹⁰¹

Of course, identifying a theory—or theories—of change does not guarantee that a particular intervention will achieve the desired outcome. Many questions around viability cannot be answered until a system actually is in place. But considering theory of change along with other substantive criteria does provide a framework for answering questions around how to design a certification system so that it is most likely to be effective. Next, we turn to these design choices.

IV. DESIGN CHOICES

Suggesting the idea of a certification body is only the beginning. Working from some operative theory of change and other substantive considerations, any certification approach then requires navigating a number of design choices. Here, we discuss five such choices, any of which can affect the nature and scope of certification.

A. PRESCRIPTIVE VS. DESCRIPTIVE

Certification regimes fall along a spectrum from descriptive to prescriptive. Descriptive systems seek only to provide objective, unbiased information, leaving it to the consumer to make the ultimate decision whether to purchase a product. Diamond certifications are descriptive—*any* diamond can be certified; the certification simply provides information about a diamond’s characteristics.¹⁰² Possessing that information, the purchaser is left to make whatever choice is preferred. As a result, for a descriptive certification to be meaningful, the consumer must have some sense of what the information means and how to use it. (Of course, even a descriptive certification is not value-neutral: there was a decision on the part of the certifier about what deserved to be evaluated and what information provided to the public.)

Prescriptive certifications are more evaluative, signaling that a product is satisfactory in a particular regard or that it conforms to a particular standard.

101. Marchant, *supra* note 61, at 136 (noting that successful certification schemes must give industry something of value to incentivize participation).

102. The leading diamond certifier is the Gemological Institute of America, which assesses diamonds on the basis of their color, clarity, cut, and carat (the “4Cs”), among other characteristics. See *Sample Natural Diamond Reports*, GEMOLOGICAL INST. OF AM., <https://www.gia.edu/analysis-grading-sample-report-diamond?reporttype=diamond-grading-report&reporttype=diamond-grading-report> (last visited Apr. 6, 2022).

B Corporations, discussed in Section III.B, are an example of prescriptive certification. A private organization called B Lab confers this certification on companies that have met standards relating to social and environmental performance, transparency, and other values.¹⁰³ Prescriptive systems tell consumers or potential purchasers that an independent third-party with relevant expertise has evaluated the product or company and has approved of it in a certain respect. Certified vendors essentially receive a gold star, and consumers don't have to do their own information gathering but can simply respond to the signal certification provides.

Depending on the operative theory of change and other considerations such as capacity, resources, and legitimacy, tech certification could be prescriptive, descriptive, or somewhere in-between. In the following example, we show what a prescriptive, descriptive, and hybrid regime (such as a system that rates or ranks products) might look like for certain aspects of automated license plate readers.

ALPRs are used to alert police when a *particular* wanted vehicle is detected.¹⁰⁴ But license plate reads also can be stored away, time-stamped and geo-located, to be fished out for investigative purposes.¹⁰⁵ Many people are concerned about the storage and use of this “historical data” to track individuals’ movements over time.¹⁰⁶ This concern could be mitigated partially by automatically deleting historical data after a set period of time, known as a “retention period.”¹⁰⁷ A shorter retention period means that an agency has less ability to track a vehicle’s movements over time.

The image on the following page indicates what a prescriptive, descriptive, and hybrid certification scheme might look like for ALPRs with regard to the retention period. (Of course, an entity certifying ALPRs would consider much more than just retention periods; we focus on them here for simplicity’s sake.)

103. See *About B Corp Certification*, B LAB, <https://bcorporation.net/about-b-corps> (last visited Apr. 6, 2022).






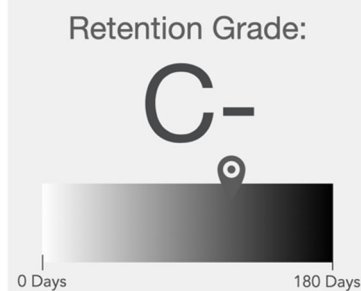
104. See *id.*

105. See *id.* at 5.

106. See *id.* at 24.

107. See *id.* at 34.

Table 2: Certification Approaches

ALPR 1: 28-day retention	ALPR 2: 120-day retention
<i>Prescriptive Certification: Retention period of thirty days or less is required for certification</i>	
 <p>ALPR 1 has met the certification condition and is certified.</p>	 <p>ALPR 2 does not meet the condition and is not certified.</p>
<i>Descriptive Certification: Certifies all products</i>	
 <p>Certification states ALPR 1's retention period of 28 days.</p>	 <p>Certification states ALPR 2's retention period of 120 days.</p>
<i>Hybrid Certification (Rating System): Certifier gives product a grade based on the length of retention</i>	
 <p>ALPR 1 receives a higher grade for a shorter retention period</p>	 <p>ALPR 2 receives a lower grade for a longer retention period.</p>

One's theory of change will influence where along the prescriptive-descriptive spectrum a policing tech certification system should land. For example, if the theory of change is to influence vendors, then the certification system would need to be more prescriptive in design. As described above, prescriptive models (including hybrid models, such as rating systems) provide

a strong branding chip for certified vendors by signaling approval of their product. On the other hand, if the goal is to influence the public and regulators, then descriptive certification, which seeks to provide objective, unbiased information, may be better suited to bridging the information gap that these groups face.

Either approach—influencing vendors or influencing the public/regulators—could address the race to the bottom. Prescriptive (and hybrid) models directly incentivize vendors to improve their products so as to receive certification or obtain a high grade or rating. (However, this assumes that the certification criteria are transparent to vendors, which most, but not all, are.¹⁰⁸) Descriptive models indirectly incentivize vendors to improve their products, as public pressure forces policing agencies to choose to purchase (or not purchase) products based on the information that certification provides.

Ultimately, our research and discussions with stakeholders revealed strong skepticism around prescriptive-type certifications for policing tech because of these systems' norms-setting requirement. Many stakeholders expressed doubt that prescriptive systems premised on influencing vendors or policing agencies would produce a normative calculus that benefited communities. Others took issue with the very idea of establishing normative standards for issues like privacy or racial justice, arguing that there was no way to achieve consensus standards on such ethical dimensions. Stakeholders have different conceptions of what makes a product “ethical,” and the communities in which technologies are deployed may well disagree with a certification entity's conclusions and prefer to make their own determinations. Even if some imperfect baseline was established via a transparent process, consumers may misunderstand or put too much stock in what prescriptive certification represents—indeed, in the context of eco-certifications, there is a long-standing problem of “greenwashing”: the use of labels or certifications that misleadingly suggest that a product is environmentally friendly.¹⁰⁹

Finally, several stakeholders worried about the impact that prescriptive certification could have on criminal defendants seeking to challenge use of these technologies. Would an arrest that resulted from an agency's use of a certified product receive a thumb on the scale for its validity? As a result, many

108. Most certification regimes are transparent, but some (such as the Motion Picture Association of America's film rating system) apply *general standards*, as opposed to *precise rules*. This can undermine transparency by obfuscating the reasons for the entity's certification decisions. See Jeanne C. Fromer, *The Unregulated Certification Mark(et)*, 69 STAN. L. REV. 121, 142 (2017).

109. See HAMISH VAN DER VEN, BEYOND GREENWASH: EXPLAINING CREDIBILITY IN TRANSNATIONAL ECO-LABELING 64 (2019).

urged that any prescriptive certification would need to provide explicit disclaimers around the weight to give to its labeling in criminal adjudications.

Although stakeholders raised various concerns with prescriptive certification, significant consensus emerged around the need to inject the policing tech ecosystem with more reliable and objective information about these products. Law enforcement representatives described how the product information vacuum has forced them to rely on a sort of inter-agency rumor mill when seeking information about the utility of certain products. Civil liberties advocates, researchers, and government officials likewise bemoaned the absence of a trustworthy source for even basic information about these tools. Descriptive certification, with its emphasis on centralizing neutral information in a single entity, has the potential to fill these gaps. And because descriptive certification aims to disclose rather than evaluate information, it also largely can avoid the normative consensus traps that face prescriptive systems and hold space for different communities' needs and values by allowing jurisdictions to reach their own ultimate conclusions regarding ethical standards.

Still, descriptive systems are not without tradeoffs. They require policymakers (or the general public) to *interpret* the information disclosed. This places an evaluative burden on communities and policymakers, who, as discussed above, generally are not equipped with the expertise or tech literacy required to conduct a rigorous analysis. And without clear ratings and cross-product comparison, descriptive systems make it difficult for consumers to differentiate between products.

These concerns led some to prefer hybrid systems that both describe a particular product's qualities and provide some metric of comparison to a standard. For example, one stakeholder suggested borrowing from food nutrition labeling in which a single label both describes the nutrition content of the particular product and compares it to the recommended daily nutrient allowance. There even was a suggestion that the concerns raised by trying to certify "ethical" policing tech could be avoided by turning the entire project on its head to certify only the worst offenders, giving out stamps of *disapproval* for products that clearly are beyond the pale.

B. EVALUATING EFFICACY

How would a tech certification entity evaluate products' efficacy? This depends on a number of factors—what the theory of change is, whether the certification is descriptive or prescriptive, the availability of data upon which to base conclusions about efficacy, and the entity's resources and expertise, to name a few. Perhaps the most important factor—and the thorniest to

resolve—is how one defines “efficacy.” And defining this term carefully is essential because a certification entity’s definition can affect how vendors design their products and how those products are perceived by policymakers and the public.

First, a certification entity simply could evaluate a product’s specifications—i.e., does it do what it says “on the tin.” For example, how long can a drone remain airborne without requiring recharging? How accurately does an ALPR read a license plate? Law enforcement representatives we spoke to repeatedly observed that this information would prove quite useful in their procurement and deployment decisions. They were hardly alone; advocates likewise expressed frustration with the lack of available objective information on whether these products fulfill their basic technical promises. Many welcomed the prospect of a certification system that might step into this void and help encourage minimum viable technical standards for these policing technologies.

There are serious challenges posed by even this minimal version of efficacy review: (1) it is extremely expensive to develop test suites to evaluate these products; (2) efficacy testing always is contestable; (3) it requires some sort of apples to apples comparison across a product line, and it’s unclear if that is even as feasible with policing tech as it is with, say, vacuum cleaners; and (4) AI and ML technologies raise a host of domain transfer issues—for example, which dataset would serve as the measurement baseline (training? testing? deployment?) with pros and cons to each. Add to that the difficulties posed by the need to frequently re-evaluate in the face near-constant software and hardware updates. Some machine learning tools even continuously learn in the field—in essence, as the model ingests deployment data, its pattern regulation algorithm changes. Even without the bureaucratic obstacles facing hard law, it would be challenging to design a certification system that is flexible enough and has the capacity to assess such continuous product change.

Some stakeholders suggested some of these issues could be addressed by placing the burden back on the vendor, for example, by requiring self-evaluations and self-attestations of conformity to a standard rather than requiring the certifier to conduct the testing itself.

Even assuming the practical problems with an approach that measures basic technical efficacy could be resolved, there still are limits to its utility as the sole measure of efficacy. For example, the accuracy of ALPR reads is surely an important consideration, but it says relatively little about whether deploying ALPRs would be *useful* in achieving public safety. Many experts felt strongly that efficacy is a useless metric unless it communicates something about the actual operational value of the tool.

Second, a certification entity might evaluate a product's impact on crime-fighting by attempting to tie product use to policing metrics such as cases cleared or crime deterred. This, too, may prove to be vital information, especially if this efficacy evaluation enabled comparisons across product lines to determine which type of tool actually is more likely to have a positive impact on crime-fighting. For example, both face recognition and fingerprint identification are biometric tools used to identify suspects. Imagine a certification system that was able to aggregate and report out data on successful suspect identifications by face recognition and fingerprint with breakdowns by agency or jurisdiction, perhaps as compared to system cost. This kind of comparative information could guide agencies in choosing which tools to procure or inform legislative decisions around law enforcement budget allocations. It also could inform and empower advocacy campaigns by providing some factual basis for what affects crime-fighting and what doesn't.

But to conduct such an analysis, the certification entity must have *access to data*. Many agencies don't generate such data in the first place, let alone turn it over to independent researchers. And even if the data is generated, answering these questions as an empirical matter can prove very difficult. If (and it is a big "if") one measures crime fighting by the number of crimes reported to police, how is causation established? That is, how can one be sure that changes in the crime rate are attributable to the vendor's product? There are methods of determining causality in the social sciences, but the challenges to doing this are not insignificant.

Third, and most ambitiously, tech certification could evaluate a product's overall effect on public safety. This raises a litany of thorny questions. How does one define and then measure public safety? The number of cases closed? The amount of crime deterred? Community surveys? What about the *positive* civil rights impact of technology, such as the use of technology to constrain officer discretion or enable better oversight?

Using ALPRs again as the model, the graphic below visualizes these three approaches:

Table 3: Approaches to Evaluating Efficacy

<p>Evaluate product specifications: For example, evaluate the accuracy of ALPR plate reads or the algorithmic bias of face recognition</p> <p>Daytime Accuracy: Pass (95%)</p> <p>Nighttime Accuracy: Pass (90%)</p>																	
<p>Evaluate impact on policing metrics: For example, evaluate clearance or arrest rates</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th colspan="3"><u>Clearance Rates</u></th> </tr> <tr> <th colspan="3">Based on data from 20 agencies, Jan. 2023–Dec. 2023</th> </tr> <tr> <th></th> <th>Property & Vehicle Offenses</th> <th>Violent Offenses</th> </tr> </thead> <tbody> <tr> <th>With ALPR</th> <td style="text-align: center;">30%</td> <td style="text-align: center;">50%</td> </tr> <tr> <th>Without ALPR</th> <td style="text-align: center;">24%</td> <td style="text-align: center;">52%</td> </tr> </tbody> </table>			<u>Clearance Rates</u>			Based on data from 20 agencies, Jan. 2023–Dec. 2023				Property & Vehicle Offenses	Violent Offenses	With ALPR	30%	50%	Without ALPR	24%	52%
<u>Clearance Rates</u>																	
Based on data from 20 agencies, Jan. 2023–Dec. 2023																	
	Property & Vehicle Offenses	Violent Offenses															
With ALPR	30%	50%															
Without ALPR	24%	52%															
<p>Evaluate overall impact: Measure the overall impact on public safety, however conceived</p> <div style="text-align: center; margin-top: 20px;"> </div>																	

There is one final possibility that shifts the burden of proof to vendors and could lead to far more available information: certification could set rules about *how* vendors make claims about product efficacy. For example, a certification entity could require that vendors only make efficacy claims that have been vetted by independent researchers. Or it could require that vendors publicly disclose all data upon which efficacy claims are based, opening such claims up to public scrutiny. In this vein, certification could enforce a sort of “truth in

advertising” requirement, similar to requirements enforced by the Federal Trade Commission. Alternately, certification even could tell vendors what they *must* advertise on the tin, including the nature of oral representations they can make in marketing their products—akin to the requirements that prescription drug labels and advertisements list certain warnings and precautions.¹¹⁰

C. “USE” CASES

One of the great challenges of certifying policing technologies is whether to certify only the product in the abstract or to take account of particular uses of the product. Some certification schemes are contextual, others are not. Cheese, for example, might be certified as Kosher, but that does not preclude putting it on a bacon cheeseburger. On the other hand, Leadership in Energy and Environmental Design (LEED), a green building certification program, only certifies entire buildings as eco-friendly; it does not matter if all “green” materials were used, it is the way in which these materials come together into a building that counts.¹¹¹

When it comes to policing tech, context is of great importance. The ethical implications of a policing technology turn largely on two contextual use factors. First there is the issue of how individual agencies choose to use the particular product. The very same ALPR can be used by one agency only to detect vehicles wanted in connection with serious felonies but by another to generate fines and fees revenue, which fall most heavily upon predominantly minority neighborhoods. Second, there is the issue of how a technology is used in conjunction with *other* technologies—that is, how a technology integrates into a larger *system*. For example, ALPRs have been used in conjunction with aerial surveillance to enable more precise tracking of vehicles’ movements.

In short, certifying uses is difficult. They are very dependent on both the individual and systemic contexts of a given jurisdiction. To truly prove valuable, some have argued that a certification agency would have to certify products for different uses, in different combinations, in different jurisdictions. Both the decision to certify use cases, and its implementation, pose difficult challenges. Here are a few potential routes a certification entity might take in addressing use cases.

110. See Michael J. Lopez & Prasanna Tadi, *Drug Labeling*, NAT’L CTR. FOR BIOTECHNOLOGY INFO., <https://www.ncbi.nlm.nih.gov/books/NBK557743> (Aug. 19, 2021); *Drug Advertising: A Glossary of Terms*, U.S. FOOD & DRUG ADMIN., <https://www.fda.gov/drugs/prescription-drug-advertising/drug-advertising-glossary-terms> (last visited Apr. 6, 2022).

111. See *Green Building 101: What is LEED?*, U.S. GREEN BLDG. COUNCIL, <https://www.usgbc.org/articles/green-building-101-what-leed> (Dec. 16, 2020).

1. *Don't address use cases*

The first option is simply to ignore use cases. For example, certification of ALPRs could assess devices on the basis of plate read accuracy and data security, while sidestepping the questions of how, for what purpose, and in what combinations agencies use ALPRs.

The value of even such a limited approach should not be discounted. It would be valuable to have a credible, independent entity evaluate how accurately an ALPR reads a license plate, how well a predictive policing algorithm performs, or how biased (or unbiased) a facial recognition system is. Indeed, this is why the NIST tests and ranks the accuracy of face recognition algorithms. It would make little sense for each individual jurisdiction to make such assessments on its own.

There are additional benefits to this approach. A certification scheme that ignored use cases would be far easier to design and implement. And, for better or for worse, it would leave it to local policymakers to decide which use cases and combinations were permissible.

Still, when it comes to policing tech, how it is used is often every bit as important as whether it works when it is used. An algorithm that is free of racial bias could be used by agencies in a way that gravely exacerbates racial disparities (for example, for the purpose of enforcing low-level drug offenses). At present, there is little transparency around, let alone local regulation of, how agencies use policing technologies. In many (and perhaps most) jurisdictions, if the certification entity were not addressing use cases, no one would be. Many experts we spoke with questioned whether a certification system would provide any meaningful value if it did not address use cases.

2. *Certify products, addressing use cases indirectly through product design*

Second, without certifying use cases directly, certification could influence product design, which in turn can affect use cases.

For example, certification could be conditioned on the implementation of features that encourage or require agencies to be transparent about uses—both individual product uses and use in combination with other tools. If, for example, the concern is that agencies will use drones to surveil protests and other expressive activity, vendors could be required, as a condition of certification, to create transparency portals—that is, online portals disclosing information about police use of technology—through which agencies could (or must) disclose the time and flight path of each drone flight. In this way, the public would have the tools to draw conclusions about uses on their own. Also, the fact that the information would become publicly available might cause policing agencies to be more careful about their uses.

But there are limits to this approach as well. Transparency is, of course, vitally important to the effective regulation of policing agencies. Yet for transparency to lead to sensible use limitations, action still is required—by policymakers and regulators enacting reforms, by communities and civil society groups making demands of agencies, by aggrieved citizens challenging agencies' actions in court, and so on. Transparency may well lead to such efforts, but this cannot be taken as a given.

Alternatively, certification of a product might require vendors to implement design safeguards that restrict the ability of agencies to engage in certain problematic uses. For example, one way to curtail agencies' ability to conduct location tracking using ALPR historical data would be to design the device such that data was automatically deleted after seven days. Such features are, in a sense, self-auditing.

Even with this approach, though, some uses may be difficult to address through product design. Suppose that a certification entity wanted to limit the use of historical ALPR data, allowing its use only in the investigation of serious offenses. How is a vendor to design its product to allow use of historical data for serious offenses but disable agencies from running historical searches to investigate minor vandalism or graffiti? One answer is that the software could simply ask the user what the purpose of the historical search was and record that information. This, combined with a transparency mechanism, might do the trick—although there are of course always some lingering questions about the candor of all users and agencies.

3. *Directly certify use cases*

Third, the certification entity could certify use cases directly—that is, conclude that a product is certified for a specific intended purpose, when used in a specific intended way. For example, an ALPR could be certified for use in connection with the enforcement of felony offenses through the use of hotlist alerts but not certified for use in low-level enforcement. Certification also might limit the use of a product in conjunction with other technologies.

In such a scheme, the certification entity could play one of two roles. It might simply state the use cases and combinations for which a product is certified, leaving it to communities and policymakers to ensure the local agency user complies with the restrictions.

Alternatively, a certifier could enforce compliance with certified use cases. The entity might require vendors to regulate agency use through terms of service, for example. Or the entity could certify products agency by agency—i.e., certify an ALPR for use by the Whoville Police Agency because it has adopted appropriate use policies and training protocols, but not for the

Whereville Police because they have not. However, this approach would entail significant expense and, absent a vigorous program of compliance review, may not be successful anyway.

An entirely different approach to the problem of use would be to issue non-certification for certain use cases where the costs outweigh the benefits or cannot be adequately mitigated through design safeguards or other restrictions. And like an FDA drug label, tech certification labels could come with warnings about the potential risks of any non-certified uses. This approach also could be applied to target the issue of systemic use risks—the label could provide warnings about the risks of combining certain technologies, just like drug labels may warn about combining drug use with alcohol. And still another option might be certifying whether the user is qualified to use a given technology.

Table 4: Options for Addressing Use Cases

Don't address use cases		<ul style="list-style-type: none"> • Pros: Ease of design and implementation • Cons: More limited value
Address use cases through design	Design features that create transparency/accountability around agency uses	<ul style="list-style-type: none"> • Pros: Information-forcing • Cons: These features may not lead to substantive change
	Design features that restrict agency uses	<ul style="list-style-type: none"> • Pros: Limits use cases without auditing • Cons: Impractical for certain use cases
Certify use cases	Certify products for specific use cases	<ul style="list-style-type: none"> • Pros: Gives guidance to communities • Cons: Lack of enforcement mechanism
	Certify products for specific use cases + enforcement	<ul style="list-style-type: none"> • Pros: Effective at addressing many use cases • Cons: High cost

D. SUBSTANTIVE DESIGN STANDARDS

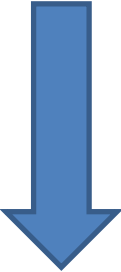
Both descriptive and prescriptive certifications apply substantive standards. In prescriptive certification, a product passes or fails based on those standards. But even descriptive systems incorporate substantive standards. Gem certification, for example, relies on substantive standards to determine whether a gem should be classified as pink or red. Likewise, a policing tech

certifier would need to decide which traits of a technology to evaluate, such as data retention, accuracy, and the like.

Substantive standards are yet another design choice, and careful thought must be given to how those requirements are designed. Should certification be directed towards giving agencies and jurisdictions choices, or should those choices be made by the certification entity?

Suppose, for example, that a certification entity determined that ALPRs should be evaluated on whether they include a transparency portal through which agencies disclose information about their ALPR use to the public. The question then arises whether certification should make the portal’s use mandatory for agencies, or whether the tool should just be part of the device, but its use by any given agency wholly voluntary. Then, even in the latter case, there is the question of whether the certification agency should include “nudges” to encourage agencies to use the portal. Nudges use design architecture to encourage users to make better decisions. How options are presented to users and which ones are enabled or disabled by default may have a profound influence on the decisions an agency ultimately makes.

Table 5: Examples of ALPR Safeguards

<p>Choice: The vendor includes a transparency portal for agencies to use <i>if they so choose</i>.</p>	 <p><i>Stronger Requirement</i></p>
<p>Choice + Nudge: The transparency portal <i>is enabled by default but can be disabled</i> by the agency.</p>	
<p>No Choice: The transparency portal is included and there is <i>no way to disable it</i>.</p>	

At first glance, the “No Choice” safeguard might seem best. Agencies are left with no choice but to include the safeguard or meet whatever substantive standard the certification agency puts in place.

The reality is more complex, in large part because substantive design choices interact with stakeholder buy-in for the certification system—an issue we discuss further in Sections IV.A–B. For example, suppose that a certification entity required vendors to use the “No Choice” safeguard. Each vendor then will decide whether to get certified and comply with this strong restriction. The basis for the vendor’s decision will depend in great part on whether the certifier has market power. If the certification standard has been adopted widely by agencies and industry, the vendor may have little choice but

to acquiesce in the “No Choice” safeguard. If, however, the certification entity is an upstart, or the vendor faces brisk competition from another vendor that does not get its products certified, the vendor may well decide to forego certification. If enough vendors forego certification, the impact of the certification scheme may be diminished.

One further point to consider is that a certifier’s substantive requirements can limit the options available to regulators and communities—products become “one size fits all.” This is hardly unique—consider, for example, the existence of federal laws that set uniform minimum standards across the United States (e.g., federal labor law and the federal minimum wage). Yet there are costs to this approach. If communities feel that certification fails to strike the right balance, they won’t be amenable to following the guidance of certification. Alternatives might be to have local or statewide bar-setting or to outsource substantive standard development to trusted expert groups.

E. INSTITUTIONAL DESIGN OF CERTIFICATION ENTITIES

Certification regimes differ markedly in the extent to which they are independent from industry and include community stakeholders. In some regimes, industry dominates the standards-setting and certification process, while other entities seek to ensure balanced power-sharing. These contrasting approaches are exemplified by the two certification regimes discussed below: the International Sustainability and Carbon Certification and Fairtrade.

Table 6: Governing Certification: Two Contrasting Approaches

	
<p>The International Sustainability and Carbon Certification is governed by a 150-member association. 90% of its members are producers, processors, or others involved in the supply chain. The organization's Board consists only of industry representatives and two researchers.¹¹²</p>	<p>Fairtrade is governed by the organization's General Assembly and Board. Producers and national Fairtrade organizations (which raise awareness and administer the standard) have equal representation in the organization's General Assembly and Board, leading to balanced power-sharing.¹¹³</p>

If the theory of change envisions vendor engagement with certification as the lever, then industry requires a significant place at the table. Vendors scarcely can be expected to participate in a certification scheme that doesn't adequately represent their interests.

Whereas if the theory of change envisions legislators or the public as the target audiences, then there may be less of a need to have vendors fully on board. To be sure, some certification entities evaluate products without the vendors' cooperation—for example, an entity focused on evaluating household products might purchase a product independently, before rating it or giving it a seal of approval. That, in a sense, is how Consumer Reports operates.¹¹⁴

This approach would face unique difficulties in the current policing technologies marketplace. Most policing technologies cannot be bought from a store shelf. Some agencies we spoke with, particularly federal law enforcement, cited national security concerns with disclosing policing tech information. The vendor also often has (or least, claims) proprietary reasons to keep product information under wraps, backed by trade secret/IP law. Consequently, evaluating such products may require the vendor to submit

112. GREENPEACE, *DESTRUCTION: CERTIFIED* 54 (2021).

113. *Our General Assembly and Board*, FAIRTRADE INT'L, <https://www.fairtrade.net/about/ga-and-board> (last visited Apr. 6, 2022).

114. *See Research and Testing*, CONSUMER REPS., <https://www.consumerreports.org/cro/about-us/what-we-do/research-and-testing/index.htm> (last visited Apr. 6, 2022).

willingly to the certification process. Otherwise, the entity would be forced to conduct product evaluations on a slim public record. Even so, it is hard to imagine the development of a system that cuts vendors out entirely.

Nonetheless, there are obvious dangers if certifiers becoming too cozy with industry. Overrepresentation of industry in certification schemes can lead to capture, resulting in ineffectual standards and lax auditing.¹¹⁵ Moreover, capture by industry comes at the expense of other stakeholders—such as representatives of the communities that are most affected by policing. Balanced representation within the certification entity and its governing body would be crucial in ensuring that all stakeholders' interests are accounted for adequately.¹¹⁶

There are many ways in which a certification entity could implement mechanisms for public participation. For example, an entity might implement a notice and comment period during which interested members of the public could give feedback regarding proposed standards. Another possibility is the creation of a grievance process, by which the public could file complaints in relation to harmful uses of policing technologies—this information could guide future standards-setting and certification decisions. Such mechanisms might afford affected communities meaningful opportunities to participate in the standard-setting and certification processes and ensure that industry players with deep pockets and the time to dedicate to lobbying do not end up dominating the process.

F. PUBLIC OR PRIVATE

Finally, there is a choice to be made regarding whether certification ought to be administered by a *private* or *public* entity. Most certification regimes are administered privately. That is true of B Corporations, LEED, Fairtrade, and many others. Still, there are some notable exceptions, such as Energy Star, the energy efficiency standard administered by the U.S. Department of Energy.

In our research, we encountered significant skepticism around private entities administering a policing tech certification. This skepticism emerged from civil rights advocates, community activists, and tech vendors alike. Chief among these concerns was how the entity would be funded; if the answer was industry, many warned that issues of conflicts of interest and capture would be unavoidable and unmediatable. Others noted that institutional trust in policing agencies and Big Tech is low, especially from communities most impacted by policing tech, such as Black communities. Thus, for the entity to

115. See GREENPEACE, *supra* note 112, at 11.

116. See K. Sabeel Rahman & Jocelyn Simonson, *The Institutional Design of Community Control*, 108 CALIF. L. REV. 679 (2020).

have legitimacy in the eyes of the public, it cannot be seen as being in bed with either policing agencies or tech vendors. And the need for this entity to have teeth or enforcement power also counseled in favor of a public program with its penumbra of hard law in the background.

Consensus emerged that the certifier role should be played by a public entity. There is much to be said for public certification. It may engender more trust from the public and more naturally addresses concerns about the democratic legitimacy of certification.¹¹⁷ Moreover, public certification could have a profound and immediate effect on the market, especially if certification were tied to federal funding for policing agencies. Of course, this leaves certification vulnerable to the vicissitudes of politics. In early 2017, for example, the Trump administration sought to end the Energy Star program; in early 2021, the Biden administration sought to expand it.¹¹⁸

The question is whether a public approach is viable. It would take political energy to get it adopted, and the currently anemic regulatory environment suggests legislators don't have the stomach for stepping into this space. On the other hand, the existing regulatory lacuna likely is not the product of legislative disinterest, but self-interest. As discussed above, the topic of policing is both polarizing and highly salient to voters; comprehensive reform through legislation is a risk that many legislators may not be willing to take.¹¹⁹ It is precisely for this reason that legislators may prefer to offload the issue to some sort of regulatory agency or certification body. As Lisa Schultz Bressman has observed:

Congress might attempt to avoid blame for controversial policy choices by shifting them to agencies, while still claiming credit for broad solutions to public problems. In other words, Congress might aim to write just enough policy to receive a positive response for its

117. See Marchant et al., *supra* note 61, at 130; see also Hagemann et al., *supra* note 59 (discussing public-private models of certification).

118. See Nives Dolšak & Aseem Prakash, *The Trump Administration Wants to Kill the Popular Energy Star Program Because it Combats Climate Change*, WASH. POST (Mar. 23, 2017), <https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/23/the-trump-administration-wants-to-kill-the-popular-energy-star-program-because-it-combats-climate-change>; Tik Root, *Biden Administration Announces New Energy Star Standards, Plans for Emissions Targets for Federal Buildings*, WASH. POST (May 17, 2021) <https://www.washingtonpost.com/climate-solutions/2021/05/17/biden-energy-efficiency>.

119. See generally Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079, 1089 (1993).

actions, while deflecting any negative attention for the burdensome details to the agency.¹²⁰

Whether public or private, the entity would face a key capacity challenge: the type of evaluation envisioned requires diverse expertise and technical experience that currently is in short supply across the public and private sectors. Putting aside all the challenges around standing up such an entity, the question remains: who would staff such an entity?

V. CHALLENGES

Thus far, we have been considering what design choices would have to be made to get a certification body going from the ground up. But once the choice is made to proceed with a certification entity, there still will be challenges. This Part discusses some key challenges faced in setting up a certification body and suggests what could be done about them.

A. GAINING LEGITIMACY AND CREDIBILITY: PUBLIC BUY-IN

Certification systems naturally raise concerns about democratic legitimacy. Most standard-setters and certifiers either are several steps removed from direct democratic processes (if certification is run by a public agency) or are entirely separate from them (if run by a private entity).¹²¹ Consequently, whether the system is publicly or privately run, the public may feel shut out of the certification process and/or that industry has too much sway.¹²² This matters: if certification is to wield any influence over how policing technologies are designed and regulated, communities and policymakers must trust the certifier.

There are elements of certification design that can help ensure meaningful public voice and representation. As an initial step, basic transparency around

120. Lisa Schultz Bressman, *Chevron's Mistake*, 58 DUKE L.J. 549, 568 (2009).

121. See Lytton, *supra* note 67, at 569; Kenneth W. Abbott, *Introduction: The Challenges of Oversight for Emerging Technologies*, in INNOVATIVE MODELS FOR EMERGING TECHNOLOGIES (2014); Doris Fuchs, Agni Kalfagianni, & Tetty Havinga, *Actors in Private Food Governance: The Legitimacy of Retail Standards and Multistakeholder Initiatives with Civil Society Participation*, 28 AGRIC. HUM. VALUES 353 (2011) (noting that regulatory agency rule enforcement is subject to attenuated “legitimacy chains” as regulatory power is delegated to bureaucrats); Gutierrez, *supra* note 98, at 144–45 (observing that the fact that “any organization” can create a soft law system can raise legitimacy issues) ¶; Hagemann et al., *supra* note 59, at 98–99 (discussing legitimacy issues that even may face public approaches to soft law governance).

122. See Marchant et al., *supra* note 37, at 9.

the certification process can foster public legitimacy and credibility.¹²³ This ideally occurs at every step of the process—from initial standard-setting to individual certification decisions. Transparency, in turn, can breed accountability. For example, some have argued that certification entities should publish the reasoning behind their certification decisions, creating a body of binding precedent that enhances procedural fairness.¹²⁴

Certification systems can, and should, go a step further by actually soliciting and incorporating public input on their certification standards and process. For example, the Sustainable Forestry Initiative, which certifies sustainable forestry practices in the United States and Canada, subjects its certification standards to review every five years in a process that includes an opportunity for public review and recommendations.¹²⁵ Another major player in the certification world, Underwriters Laboratories, opens its standards creation and revision process to any interested party and actively empanels a broad set of stakeholders across industry, technical experts, and consumers to review all suggestions.¹²⁶ Its panels also request and respond to public comments, and it publicly releases its standard-setting activities.¹²⁷ When designed with such open participation guarantees, voluntary certification may in fact be “more directly democratic than the state regulatory apparatus.”¹²⁸ Participatory mechanisms also can address the problems of capture and representational imbalances, as discussed in Section III.E. But just as important, they are a means to hold the certifier itself accountable and enhance its standing among the relevant stakeholders.

In short, public legitimacy presents a difficult but not insurmountable challenge for certification systems whether they are administered by private entities or public agencies.

B. ACHIEVING UPTAKE: AGENCY AND VENDOR BUY-IN

Successful certification systems typically provide value to both the producers and consumers in the target marketplace. The ethical policing tech

123. *Cf. id.* at 12 (explaining that a mechanism for making soft law more effective and credible may include “transparency in demonstrating compliance”).

124. Fromer, *supra* note 108, at 190.

125. Cary Coglianese, *Environmental Soft Law as a Governance Strategy*, 61 JURIMETRICS J. 37–38 (2020).

126. Lytton, *supra* note 67, at 569.

127. *Id.*

128. Tracey M. Roberts, *The Rise of Rule Four Institutions: Voluntary Standards, Certification and Labeling Systems*, 40 ECOLOGY L.Q. 107, 140 (2013); *see also* Gregory N. Mandel, *Regulating Emerging Technologies*, 1 L. INNOVATION & TECH. 75, 90 (2009) (“Broad stakeholder outreach and dialogue can bring credibility, new ideas, current information, continual feedback, and public trust to a governance system.”).

marketplace presents an interesting wrinkle in that the consumers are bifurcated: agencies, who are (typically) the buyers, and the public, who is the end-user (or end-used-upon). At present, the public largely is cut out of the producer-consumer relationship. Vendors deal directly with agencies, and this feedback loop mostly ignores ethical harms. The purpose of certification is to inject ethical concerns into this loop by explicitly evaluating them and thereby making them marketable. Success then depends on the degree to which key stakeholder groups—tech vendors, agencies, the public—value the information certification provides. As discussed above, value to the public will hinge on legitimacy and credibility issues.

For agencies and vendors, the value calculus raises different, albeit related, questions. Will agencies find enough value in certification’s potential to reduce public backlash to choose certified products even when legislation or their own policies do not require it? Some law enforcement representatives we spoke with indicated this incentive may not be powerful enough to cause agencies to alter the status quo. Similarly, will a critical mass of vendors deem there to be sufficient brand value from ethical labeling to undergo certification? Or will the lack of a requirement on the agency side to purchase certified products defeat buy-in? These buy-in issues may dictate, or at least greatly impact, the design of the certification system. For example, a certification entity might choose to design a prescriptive certification system rather than a descriptive one to ensure vendor buy-in to the system.

Or take setting certification criteria for ALPR data retention. Standards that are too rigorous might impede initial adoption of the standard by vendors concerned by limiting their customers’ choices. Interestingly, if a certifier does have market power, vendors may have an incentive to encourage it to raise certification standards in order to entrench their own market power.¹²⁹ For example, an ALPR vendor might favor a standard requiring advanced analytics of racial and socioeconomic disparities resulting from ALPR use, a feature that upstart competitors may lack the resources to implement in their own products. However, raising the bar in this way only goes so far; monopolization of a product category by a vendor may stagnate innovation not only in the product’s core features but in its safeguards and accountability features as well.¹³⁰

129. For example, small watchmakers in Switzerland complain that the standard to certify a watch as Swiss-made is too rigorous and intentionally designed to shield the country’s dominant watchmakers from competition. *See* Fromer, *supra* note 108, at 150–51.

130. *See generally* Elizabeth Joh & Thomas Joo, *The Harms of Police Surveillance Technology Monopolies*, DENVER L. REV. F. (forthcoming 2022) (“When a particular technology has only a

When it comes to certification uptake by vendors and agencies, there is also something of a critical mass conundrum: buy-in by stakeholders begets buy-in, but getting over that initial hump to create a system with sufficient market power to encourage additional participation may be a Sisyphean task.

C. COMPLIANCE AND ENFORCEMENT

Certifiers face a dilemma: how does a certification entity ensure that vendors comply with certification requirements, especially over time? This is no small matter because failure to enforce certification requirements can diminish the certifier's credibility and undermine the reason for having certification in the first place.¹³¹

Enforcing certification requirements is easier said than done. Because certification typically is voluntary, certifiers must rely mostly on carrots, not sticks, to ensure compliance.¹³² (Weak enforcement may be especially acute for private certifiers; if the system were run by a federal agency, as proposed by FAS and discussed above, industry may be warier of failing to comply with a program that has the imprimatur of a government agency.)

Regardless of whether the certification entity is public or private, certification systems have developed methods of monitoring compliance that could be applied in the policing technology context. These include:

- *Tip Programs*: The certifier could set up a program to solicit tips from the public regarding violations of certification requirements. For example, if an agency's drone fleet is certified for use only in connection with active crime scenes, citizens could report that the agency was using the drones to monitor political protests.
- *Audits*: Regular audits of tech vendors and/or the agencies using their products could be a requirement of certification. (This might be part of the certifier's contract with vendors—vendors must submit to audits as a condition of using the certification mark.) For example, a certifier could require that ALPR users provide a reason for performing any historical searches. The certifier then could require the vendor to provide a representative sample of these audit trails at

sole provider, it may be of low quality: the technology may still be maturing, or the lack of competition has reduced incentives to improve it.”)

131. As Gary Marchant explains, though, enforcing certification requirements is easier said than done: “design and implementation of a cost-effective post-market surveillance system is difficult, due in large part to the ‘noise’ inherent in studying complex and diverse real-world situations.” Marchant et al., *supra* note 61, at 150.

132. *See id.* at 136; *see also* Roberts, *supra* note 128, at 146 (observing that voluntary certification systems can “encourage” compliance with their requirements but lack mandatory enforcement powers).

regular intervals to determine if the vendor's clients were running searches for impermissible purposes.

- *Sanctions:* Companies that violate certification requirements can have their certification revoked. Stakeholders we spoke to urged the use of contracting leverage to implement enforcement: agencies or vendors could incorporate clawback clauses that make ethical requirements or certification compliance part of the performance clause. And some certifiers even have sued vendors for violating requirements while using the certification mark on a theory of trademark dilution.¹³³ The gravest sanction may come from the court of public opinion—certifiers could publicize gross violations through media and public relations campaigns.

Choosing adequate enforcement and compliance mechanisms are important, but they are only part of the battle when it comes to ensuring a policing tech certification is doing its job. The other half of the battle is an issue that also stymies hard law regulation: figuring out ways for certification to keep pace with these rapidly changing technologies. Still, with the right design thinking and vendor cooperation, there likely are ways to implement regular monitoring. And even if the certification merely set a regular re-certification schedule (annually or every two years) rather than some kind of close-to-live monitoring, this would represent a significant improvement over the status quo in which there are no rules or requirements around product auditing.

D. FENDING OFF REGULATION

As discussed above, certification both can *complement hard law systems* (or fill gaps in them) and *facilitate the adoption of hard law*. The problem is that creating a certification body also may have the exact opposite effect: warding off the adoption of hard law.¹³⁴ By signaling to regulators and the public that the problems presented by these products are being addressed, certification systems can disincentivize further regulatory action. For example, in response to public backlash about violent video game content, tech companies created

133. See Trevor T. Moores & Gurpreet Dhillon, *Do Privacy Seals in E-Commerce Really Work?*, ACM (Sept. 28, 2021), <https://cacm.acm.org/magazines/2003/12/6646-do-privacy-seals-in-e-commerce-really-work/fulltext>.

134. See Carlos Ignacio Gutierrez & Gary Marchant, *Soft Law 2.0: Incorporating Incentives and Implementation Mechanisms Into the Governance of Artificial Intelligence*, OECD.AI: POL'Y OBSERVATORY (July 14, 2021), <https://oecd.ai/en/wonk/soft-law-2-0> (discussing reasons why organizations comply with soft law programs and observing that “[o]ne incentive is to avoid inflexible hard law requirements that would otherwise kick-in”).

a rating system that successfully placated federal and state lawmakers “who were pitching a variety of more formal restrictions on youth access to video games.”¹³⁵ Today, this industry-developed ratings system remains the “primary governance mechanism in this arena.”¹³⁶ In fact, scholars have noted that certification’s potential to stave off hard law often serves as a key incentive for organizations to submit to these systems.¹³⁷

There are two things that can be said here. The first is that a successful certification system may eliminate the need for hard law. That arguably was the case with the video game example. (Studies show that children “spend less time playing violent video games when their parents use the rating system to guide purchases and set rules for video game play.”)¹³⁸ And indeed, certification may be better in some instances than regulation. Unlike the traditional regulatory process, certification has the ability to bring together a broad coalition of stakeholders and subject matter experts in a non-adversarial process to devise the rules of the road. Lest we forget, legislative efforts are subject to watering down from industry interest groups and partisan divisions alike. Through its multistakeholder and more flexible process, certification presents an opportunity to set a higher or more precise bar for the industry standard.

However, not all the problems with policing tech can be solved by certification alone. For certification to be viable, it must not undercut government regulation of the police. Rather, certification should be designed in a way that *stimulates* and serves as a model for the development of hard law.

First, the certifier could focus on areas in which a lack of information has most impeded effective regulation. For example, very little is known about how useful ALPR historical data is to policing agencies. A certifier could require vendors to produce aggregated statistics about historical data use—how often agencies use data older than thirty days, for example—which could provide valuable insights to lawmakers.

Second, the certifier could itself engage in advocacy. Consumer Reports, for example, has an advocacy arm that lobbies for consumer protections on a number of fronts. A policing tech certifier might lobby for more hard law

135. Adam Thierer, *Soft Law in U.S. ICT Sectors: Four Case Studies*, 61 JURIMETRICS J. 79 (2020).

136. *Id.*

137. See Gutierrez et al., *supra* note 121, at 137 (“Firms can endeavor to sidestep hard law by developing soft law that eases society’s reservations about their products or services.”).

138. IOWA STATE UNIV., *Video Games Ratings Work, if You Use Them*, SCI. DAILY (Jan. 25, 2017), <https://www.sciencedaily.com/releases/2017/01/170125145805.htm>.

regulation of policing tech and could draft model legislation requiring agencies to use the safeguards that the certifier requires vendors to implement.

Although a policing tech certification entity should be mindful of warding off regulation, making effort to incorporate design choices that would support or complement hard law, it is not a reason to derail further exploration. As several stakeholders pointed out, even without any soft law measures on the horizon, policymakers thus far have abdicated their responsibility for regulating policing technologies.

E. NORMALIZING TECHNOLOGIES

There also is a concern that any governance system that engages with these technologies in any way—even if it is to try to mitigate the ethical harms they present—risks validating or further entrenching their use. For this reason, some believe that the only way to mitigate the harms of law enforcement use of these tools is to ban them outright.

But this argument rests on a few questionable premises: (1) that these tools are not already being normalized, (2) that there are not sufficient public safety benefits to extract from these tools assuming the necessary safeguards are in place, and (3) that there is sufficient political and public will to enact widespread bans.

Despite significant advocacy campaigns to ban FRT, one of the most high-profile surveillance tools, fewer than two dozen jurisdictions across the country have passed bans.¹³⁹ And this movement is up against majority opinion—a Pew Research Center poll found that 56% of Americans trust law enforcement will use this tool responsibly. In the meantime, law enforcement use continues unchecked.

Still, FRT is only one technology, albeit an understandably controversial one; believing that all policing technology would be banned is a form of magical thinking. The status quo is a world in which police are using these technologies while regulators are sitting on their hands. Certification at least presents a potential path forward to a world in which regulators have the information and motivation required to act and agencies are incentivized to acquire tools that are designed with safeguards in place to protect civil rights and liberties concerns. And a certification system need not certify every technology. It may very well decide that there are some tools that simply are too harmful or risky to merit evaluation. In doing so, certification could create

139. *Map*, BAN FACIAL RECOGNITION, <https://www.banfacialrecognition.com/map/> (last visited Jan. 27, 2022).

differentiation in the marketplace, serving as a mechanism to cut out the worst offenders.

F. CREATION OF A CERTIFICATION MARKET

Finally, it bears mentioning that the creation of one certification entity potentially can create a market for others.¹⁴⁰ That is, one certification scheme can beget additional ones, especially as industry backs competing schemes with weaker standards, allowing them to continue their current practices but with a claim to ethical certification.¹⁴¹ For example, there are so many eco-labels, of such varying quality, that an entire platform has been created just to help consumers and vendors distinguish between them.¹⁴²

There is no obvious answer to this other than (1) to back a strong scheme with sufficient publicity as to what is meaningful and what is not and (2) to ensure buy-in from a broad set of stakeholders at the outset of creating the regime.

VI. CONCLUSION

This Report has weighed the merits and challenges of a certification regime. At this point a reader may feel the issues are very complicated and that making such a regime work would be a difficult task. We don't disagree. For example, it would be difficult for a certification entity to keep up with the rapid pace of change, especially in the context of machine learning technologies that constantly evolve in the field. The very purpose of this study was to present a set of arguments and considerations for outside consumption.

It may be worth stepping away from the trees, however, to look back at the forest. What is it that certification can accomplish, and what must be avoided?

For certain, certification should not function as a permission structure for simply acquiring new technologies. We do not want agencies or policymakers to co-opt certification as a seal of approval or as a means to dodge criticism from concerned citizens. This is the single greatest concern expressed by the many privacy and civil rights advocates we interviewed. For tech certification to be viable, this concern must be addressed fully.

Similarly, the goal of certification is not to make hard choices for communities and policymakers but to give them the tools to make those

140. See Fromer, *supra* note 108, at 167.

141. See *id.*; GREENPEACE, *supra* note 112, at 9.

142. See *About*, ECOLABEL INDEX, <http://www.ecolabelindex.com/about/> (last visited Jan. 27, 2022).

choices themselves. As we have said, communities have different needs and values, and a commitment to the notion of policing as a democratic enterprise requires honoring those differences.

The hope is that certification might, rather than displacing community choice, facilitate it, while proving a trusted informational voice in decision-making. From our research and discussions, there emerged one universal revelation: there is a crying need for more information about these technologies and an impartial source to provide it. Certification is one way to meet this need, and in doing so, it might help all stakeholders make better decisions and come to an informed consensus—to know the right questions to ask to, and demands to make of, their policing agencies. One hopes policymakers would use certification not as a rationale for a decision already made but as a tool to gather and interpret all of the relevant facts so that they can reach informed conclusions. One hopes that it would lead vendors to compete to out-innovate each other on privacy protections, on transparency, or on mitigating bias.

This is, to be sure, a tall and optimistic order. But it is a far better vision of policing technology than what exists today. It is unclear whether certification ultimately is deemed a valuable approach—although many stakeholders expressed agreement that there is a pressing need for more objective information about policing technology. However, what is clear is that the status quo is unacceptable.