

COLUMBIA LAW REVIEW FORUM

VOL. 125

JANUARY 31, 2025

PAGES 1–28

POLICE TECHNOLOGY EXPERIMENTS

*Elizabeth E. Joh**

Police departments often adopt new surveillance technologies that make mistakes, produce unintended effects, or harbor unforeseen problems. Sometimes the police try a new surveillance technology and later abandon it due to a lack of success, community resistance, or both. Critics have identified many problems with these tools: racial bias, privacy violations, opacity, secrecy, and undue corporate influence, to name a few. A different framework is needed. This Piece considers the growing use of these algorithmic surveillance technologies and argues that they function as experiments on human subjects. Such technology experiments result in police reliance on automated systems to engage in investigative stops and consensual encounters and to increase police presence and surveillance in a community. In acting as experiments on human subjects, these tools often function poorly. Moreover, ethical considerations that are common in the conventional human subjects–research context are entirely absent, even though the new technologies involve uncontrolled experiments on people. And because these algorithmic surveillance technologies are often adopted in low-income communities of color, they raise particularly sensitive concerns about ethics and experimentation borne out by historical experience. By understanding the adoption of new algorithmic surveillance tools as experiments on human subjects, we can develop prospective controls and methods of evaluation for the use of these tools by police, ones that balance innovation with ethical responsibility as artificial intelligence becomes a normal part of police investigations.

* Professor, University of California, Davis, School of Law (King Hall). Many thanks to Nila Bala, Jack Chin, Eric Fish, Tom Joo, Chimène Keitner, and the librarians of the Mabie Law Library.

INTRODUCTION

Police departments often adopt new surveillance technologies that make mistakes, produce unintended effects, or harbor unforeseen problems. In 2011, *Time Magazine* touted the predictive policing program of Santa Cruz, California, as one of the best inventions of the year.¹ Almost a decade later, Santa Cruz became the first American city to ban the very same technology.² Sometimes the police try a new surveillance technology and later abandon it—due to a lack of success, community resistance, or both. Critics have pointed out that police departments’ use of these technologies can lead to many problems: racial bias, privacy violations, opacity, secrecy, and undue corporate influence, to name a few.³

A different framework is needed. This Piece considers the growing use of these algorithmic surveillance technologies and argues that they function as *technology experiments on human subjects*.⁴ Such technology experiments result in police reliance on automated systems to engage in investigative stops and consensual encounters and increase police presence and surveillance in a community. Viewed from this perspective, these tools often function poorly. Police departments use public resources to test out these new technologies with few guidelines or controls.⁵ When

1. Lev Grossman et al., The 50 Best Inventions, *Time* (Nov. 28, 2011), <https://content.time.com/time/subscriber/article/0,33009,2099708-13,00.html> [<https://perma.cc/5MFN-X7CB>].

2. Kristi Sturgill, Santa Cruz Becomes the First U.S. City to Ban Predictive Policing, *L.A. Times* (June 26, 2020), <https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes-first-u-s-city-to-ban-predictive-policing> (on file with the *Columbia Law Review*); see also Avi Asher-Schapiro, In a U.S. First, California City Set to Ban Predictive Policing, *Reuters* (June 19, 2020), <https://www.reuters.com/article/us-usa-police-tech-trfn/in-a-u-s-first-california-city-set-to-ban-predictive-policing-idUSKBN23O31A> [<https://perma.cc/4LND-GMD9>].

3. See, e.g., Andrew Guthrie Ferguson, Facial Recognition and the Fourth Amendment, 105 *Minn. L. Rev.* 1105, 1108 (2021) (noting that facial recognition systems “raise core police legitimacy issues around error rates, racial bias, fairness, and transparency”).

4. A note on terminology: Today, the terms “algorithm,” “artificial intelligence,” “machine learning,” “automation,” and “prediction analysis” are all used somewhat interchangeably in the social science and general audience literature, although some terms are technically distinct and others carry a controversial connotation. In this Piece, the terms “algorithm” and “automated system” are used as a “general shorthand for technologies that rely on machine learning techniques or explicitly programmed rules to inform or execute government actions.” This Piece slightly modifies the approach in Karen Levy, Kyla E. Chasalow & Sarah Riley, Algorithms and Decision-Making in the Public Sector, 17 *Ann. Rev. L. & Soc. Sci.* 309, 310–11 (2021). These terms should remain broad because, as Professor Danielle Citron has discussed, even relatively simple rules-based programs can have significant policy impacts and have altered the way governments provide services and deny benefits. Danielle Keats Citron, Technological Due Process, 85 *Wash. U. L. Rev.* 1249, 1260–63 (2008).

5. See, e.g., Hannah Bloch-Webha, Visible Policing: Technology, Transparency, and Democratic Control, 109 *Calif. L. Rev.* 917, 924 (2021) (“Quantification, data-driven tools,

these technologies go awry, communities are subjected to unjustified stops and arrests and unwarranted expansions in surveillance burdens.⁶ Moreover, ethical considerations that are common—and indeed mandatory—in the conventional context of human subjects research are entirely absent, even though the new technologies involve uncontrolled experiments on people.⁷ And because these algorithmic surveillance technologies are often adopted in low-income communities of color,⁸ they raise particularly sensitive concerns about ethics and experimentation borne out by historical experience.

The framework of experimentation provides a new approach to police departments' use of algorithmic surveillance technologies that current perspectives fail to capture. Concerns about privacy, civil liberties, bias, and technical issues provide important but limited tools of evaluation. By understanding the adoption of new algorithmic surveillance tools as experiments on human subjects, we can develop prospective controls and methods of evaluation for police use of these tools, ones that balance innovation with ethical responsibility as artificial intelligence becomes a normal part of police investigations. This Piece's framework provides an important practical perspective: Some police technology experiments should never have been implemented at all. These experiments lacked a clear hypothesis, engaged in little evaluation, or failed to minimize harms on vulnerable communities in the way human-subjects research demands. The police tested out unproven algorithmic tools on communities in ways they would never beta test equipment critical for their own safety or protection.

More broadly, the framework of experimentation helps to explain why many adoptions of algorithmic surveillance tools are harmful and warrant abandonment, even in the absence of clear Fourth Amendment violations or privacy harms. In other words, an experimentation framework would improve our approach to police departments' use of new surveillance tools.

and predictive techniques are reshaping policing [P]olice agencies often fight to conceal their technologies from the public and oversight institutions.”).

6. See Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 *Harv. L. & Pol'y Rev.* 15, 15 (2016) [hereinafter Joh, *Surveillance Discretion*] (defining surveillance discretion as the “decisional freedom” of police to decide who should be targeted for investigative focus).

7. The author has previously discussed how the ethical use of artificial intelligence in policing could benefit from a bioethics framework. See Elizabeth E. Joh, *Reckless Automation in Policing*, *Berkeley Tech. L.J. Comments* 116, 125–26 (2022), https://btlj.org/wp-content/uploads/2022/07/BTLJ-Joh_WebVersion_07-10-22.pdf [<https://perma.cc/D335-NAFN>] (arguing that testing automated decisionmaking in policing should be subject to ethical considerations).

8. Cf. Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 *Ohio St. J. Crim. L.* 503, 518 (2018) (noting “initial big data policing experiments signal a pattern to use such technologies more on poor communities of color”).

Part I introduces some of the algorithmic surveillance tools that have been adopted in ordinary police investigations. It identifies what is distinct about these tools compared to traditional methods and briefly describes the political and legal factors that have permitted these technologies to flourish. Part II outlines the framework for experimentation: what we mean by scientific experimentation and why it applies to the adoption of algorithmic surveillance technologies. Because these are experiments on people and communities, this Part introduces the bioethical considerations that are standard in human subject research and have been proposed in the field of artificial intelligence more broadly.

After Part II presents what good experiments look like, Part III then explains why many uses of new algorithmic surveillance technologies by local police function as uncontrolled and unethical human experiments. Using three recent examples of such experiments, this Part explains how the experimentation framework would have limited the adoption of these tools, evaluated the unjustified harms of these tools, and justified their prompt abandonment. The Part concludes with a framework for evaluating police technology experiments.

I. THE RISE OF ALGORITHMIC SURVEILLANCE TOOLS IN POLICING

This Part explains the many types of new technologies reliant on algorithms and artificial intelligence that local police departments use for surveillance and investigation. It then explores how these surveillance tools flourish in a sparse regulatory environment.

A. *Artificial Intelligence and Ordinary Policing*

Current police surveillance technologies share two general features: (1) They make use of the vast amount of data either directly collected by the police or by third parties that are then accessible to the police, and (2) they use algorithmic tools to sort, classify, analyze, and produce inferences from that information for criminal investigations.⁹ These features are common to the algorithmic tools that have transformed many sectors beyond policing, including healthcare, finance, and labor.¹⁰ The police, like other sectors in society, have embraced the analysis of massive amounts of digitized information to further their objectives.¹¹

9. See, e.g., Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 *Am. Socio. Rev.* 977, 979–80 (2017) (defining rising use of big data in a similar way).

10. See, e.g., Charlie Beck & Colleen McCue, *Predictive Policing: What Can We Learn From Wal-Mart and Amazon About Fighting Crime in a Recession?*, *Police Chief*, Nov. 2009, at 18, 19 (“Taking a cue from e-commerce and marketing, the professional law enforcement community began exploring innovative methods for the analysis of crime data.”).

11. See, e.g., Brayne, *supra* note 9, at 977 (“Big data analytics have been taken up in a wide range of fields, including finance, health, social science, sports, marketing, security, and criminal justice.”).

In policing, these technologies have vastly expanded the scope of what and whom the police can investigate and surveil.¹² We all leave behind streams of data in our daily lives, but without a way of sifting through that information efficiently and quickly, it is of little use to the police.¹³ AI tools help the police identify patterns and predictions that can be inferred from those data.¹⁴ Tools like predictive policing software, facial recognition tools, and social media analysis all rely on algorithmic technologies to produce results the police can act upon.¹⁵

The practice of government surveillance is not new. Indeed, the collection, recording, and classification of information about people and institutions are essential to modern societies.¹⁶ But the surveillance structures of today's society are quantitatively different in the sheer amount of information that can be collected about populations and qualitatively different in the kinds of inferences made possible.¹⁷ The most routine actions—writing texts and emails, buying groceries, paying tolls, searching the internet—can be recorded, saved, and aggregated.¹⁸ The features of today's surveillance technologies—passive, embedded into ordinary activities, low in visibility, and remote—permit collecting information on many people at once, without suspicion or interest in particular individuals.¹⁹

And while police have been adopting new technologies for a hundred years, today's surveillance technologies have dramatically expanded the powers and capabilities of the police. The reach of police surveillance is

12. See Joh, *Surveillance Discretion*, *supra* note 6, at 15 (describing how new technologies have expanded surveillance discretion).

13. Cf. Christopher Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs*, *Nat'l Inst. Just. J.*, Jan. 2019, at 37, 38 (noting that facial-image review is a "time-consuming, painstaking task, with the potential for human error due to fatigue and other factors").

14. See *id.* (exploring AI's use in facial analytics, fraud detection, and medical imagery).

15. See, e.g., *id.* at 43–44 (highlighting the benefits of AI algorithms in policing).

16. See Gary Marx, *Windows Into the Soul: Surveillance and Society in an Age of High Technology* 53–54 (2016) (discussing contemporary examples of the vast use of surveillance technologies).

17. See, e.g., Brayne, *supra* note 9, at 979–80 (summarizing sociological analyses of big data's rise in modern society).

18. See John Villasenor, *Ctr. For Tech. Innovation at Brookings, Recording Everything: Digital Storage as an Enabler of Authoritarian Governments 1* (2011), https://www.brookings.edu/wp-content/uploads/2016/06/1214_digital_storage_villasenor.pdf [<https://perma.cc/QXM9-656Y>] (stating that, "[f]or the first time ever, it will become technologically and financially feasible for authoritarian governments to record nearly everything that is said or done within their borders" if they wish).

19. See, e.g., Marion Fourcade & Kieran Healy, *Seeing Like a Market*, 15 *Socio-Econ. Rev.* 9, 24 (2017) (emphasizing how mundane information is used to create a real profile of individuals); Gary T. Marx, *What's New About the "New Surveillance"? Classifying for Change and Continuity*, 1 *Surveillance & Soc'y* 9, 12–13 (2016) (highlighting the large variety of ways that personal information is surveilled).

today both “*wider* and *deeper*”: It includes both the ability to scan populations and the power to track individuals across a range of activities.²⁰ Police investigations that examine “the digital footprints that ordinary Americans leave in nearly every facet of their lives” are commonplace.²¹ In this sense, these technologies today are not just another investigative tool. If left unchecked, automated systems employed by the police can harm communities.²²

B. *The Political and Legal Environment of Today’s Technologies*

A few particularly important factors account for the rise of algorithmic surveillance technologies in policing. These include the mismatch between Fourth Amendment doctrine and these technologies, the emphasis on data-driven policing methods and funding available for them, the influence of private technology vendors, and the lack of significant regulatory controls.

First, many of the algorithmic tools used in investigative surveillance do not trigger Fourth Amendment restrictions. The data collected may be public, like our faces, or it may be information like transactions that we have handed over to third parties. In both cases, the Fourth Amendment does not offer protection. In cases like *Carpenter v. United States*²³ and *Riley v. California*,²⁴ the Supreme Court has recognized that our digital data are protected in some circumstances,²⁵ but the extent to which those protections cover all personal information capable of digitization remains unsettled. In that environment, the police can collect a wide range of information without individualized suspicion or a warrant.²⁶

20. See Brayne, *supra* note 9, at 979.

21. See, e.g., Mike Baker, Inside the Hunt for the Idaho Killer, N.Y. Times (June 10, 2023), <https://www.nytimes.com/2023/06/10/us/idaho-university-murder-investigation.html> (on file with the *Columbia Law Review*) (noting that “law enforcement investigators have come to rely on the digital footprints that ordinary Americans leave in nearly every facet of their lives”).

22. See Detlef Nogala, The Future Role of Technology in Policing, *in* Comparisons in Policing: An International Perspective 191, 194 (J.P. Brodeur ed., 1995) (noting that “the introduction of technical innovations into the police not only affects their way of functioning and their performance, but also their public appearance and their social impact on society”).

23. 138 S. Ct. 2206 (2018).

24. 573 U.S. 373 (2014).

25. See, e.g., *Carpenter*, 138 S. Ct. at 2223 (holding that, “[i]n light of the deeply revealing nature of” cell site location information, government acquisition of information even gathered by a third party is a search); *Riley*, 573 U.S. at 403 (holding that searches of cellphones incident to arrest require a warrant).

26. See Joh, Surveillance Discretion, *supra* note 6, at 33–34 (noting how much of police surveillance lies outside Fourth Amendment scrutiny).

Second, data-driven policing has become a dominant model of policing associated with innovation and reform.²⁷ The community policing model, once popular in the 1980s, emphasized community input, institutional decentralization, and a focus on problem-solving more than on law enforcement.²⁸ But over the next two decades, experiences with community policing and its cousin, broken windows policing, revealed their shortcomings and raised questions about their success in reducing crime.²⁹ The Great Recession of 2008 also placed further pressure on existing policing practices as local agencies found their budgets slashed.³⁰ Local police departments sought to “do more with less” by relying on technologies offered by private companies that promised more surveillance power at less cost.³¹ In 2014, the then-Chief of Detectives at the Los Angeles Police Department wrote that a tool like predictive policing offered “an opportunity to prevent crime and respond more effectively, while optimizing increasingly scarce or limited resources, including personnel.”³²

Notably, federal funding to local police supports the data-driven model.³³ Although the structure of American policing is “overwhelmingly local,”³⁴ federal support is a significant source of how local law

27. See, e.g., Beck & McCue, *supra* note 10, at 19 (“Taking a cue from e-commerce and marketing, the professional law enforcement community began exploring innovative methods for the analysis of crime data.”).

28. See David Alan Sklansky, *The Persistent Pull of Police Professionalism*, *New Persps. in Policing*, Mar. 2011, at 1, 5 (highlighting the goals of community policing).

29. See, e.g., Beck & McCue, *supra* note 10, at 18 (discussing the role of predictive policing and analytics in improving the effectiveness of community policing).

30. See *id.*

31. Aaron Shapiro, *Reform Predictive Policing*, 541 *Nature* 458, 458–59 (2017) (internal quotation marks omitted) (noting that predictive policing systems “make good business sense” because “[t]hey are cheap compared to the costs of hiring full-time analysts or criminologists; no pensions are necessary”). The president of Persistent Surveillance Systems has described his service this way: “Our whole system costs less than the price of a single police helicopter and costs less for an hour to operate than a police helicopter But at the same time, it watches 10,000 times the area that a police helicopter could watch.” See Amanda Pike & G.W. Schulz, *Hollywood-Style Surveillance Technology Inches Closer to Reality*, *Reveal* (Apr. 11, 2014), <https://revealnews.org/article-legacy/hollywood-style-surveillance-technology-inches-closer-to-reality/> [<https://perma.cc/GXV8-S7ZY>] (internal quotation marks omitted).

32. Beck & McCue, *supra* note 10, at 18.

33. See, e.g., Brayne, *supra* note 9, at 1003 (noting that history of police surveillance technology adoption “reveals that many of the resources for developing big data analytics come from federal funds”); James Byrne & Gary Marx, *Technological Innovations in Crime Prevention and Policing*, 2011 *Cahiers Politiestudies* 17, 25 (English Issue) (arguing that new police technologies “are being adopted at a rapid pace, due in large part to significant financial support from the federal government”).

34. See, e.g., Rachel A. Harmon, *Federal Programs and the Real Costs of Policing*, 90 *N.Y.U. L. Rev.* 870, 876 (2015) (explaining how the American legal system “reserves general law enforcement power to the states”); William J. Stuntz, *Terrorism, Federalism, and Police Misconduct*, 25 *Harv. J.L. & Pub. Pol’y* 665, 665 (2002) (“The defining characteristic of American criminal law enforcement—the characteristic that most distinguishes it from law enforcement elsewhere in the developed world—is its localism.”).

enforcement agencies are structured. Federal support for local police departments can take the form of funds appropriated by Congress, monies shared through programs like asset forfeiture, and direct equipment transfers.³⁵

Third, private vendors of surveillance technologies have found in law enforcement agencies a ready-made market of customers for their products. Most police departments lack the resources to develop or produce the hardware or software necessary for these new tools.³⁶ As a result, services like Palantir's data analysis, Axon's body cameras and data storage, and Geolitica's predictive policing software are all offered as private sector products for sale, license, or subscription to police departments.³⁷ Police department customers present these firms with the prospect of multiyear recurring public contracts.³⁸ Eager to persuade their prospective police department customers, these companies have offered free trials, heavily discounted products, and help with applying for funds or negotiating complex public bidding processes.³⁹ As a result, however, private firms have enormous influence on police departments' use of technology; these firms make some of the most important decisions about the design, focus, and control over these technologies, rather than the police departments that use them.⁴⁰

Finally, these technologies have flourished in a legal climate in which there are few significant and comprehensive regulations.⁴¹ While the

35. Federal law allows local police to seize property linked to federal crimes and also to receive a share of those proceeds. See, e.g., 21 U.S.C. § 881(e) (2018); Harmon, *supra* note 34, at 929–36 (observing that federal programs designed to share asset forfeiture programs with local police undesirably alters local incentives and priorities).

36. See Elizabeth Joh & Thomas Joo, *The Harms of Police Surveillance Technology Monopolies*, 99 *Denv. L. Rev. Forum* 1, 7 (2022), https://www.denverlawrev.org/_files/ugd/9d4c2a_0eef152ccb64b10897f099d97e02c13.pdf [<https://perma.cc/KN39-NS4U>] (discussing local police departments' lack of resources to develop surveillance tools).

37. See *id.* at 16–17 (“For example, PredPol, Inc. (now called Geolitica) sells predictive-policing services to police departments. Another service, Shotspotter, uses a system of sensors in public places that constantly listens for and identifies the time and location of gunshots to guide police response.” (footnote omitted)).

38. Cf. *id.* at 15–19 (noting issues that arise with recurring police technology contracts).

39. See, e.g., Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 *NYU L. Rev. Online* 19, 32–34 (2017), https://nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf [<https://perma.cc/T98C-SRMA>] [hereinafter Joh, *Undue Influence*] (documenting instances of these technology firm developments).

40. See *id.* at 22 (explaining the dynamics of this influence).

41. See Nick Cumming-Bruce, *U.N. Panel: Technology in Policing Can Reinforce Racial Bias*, *N.Y. Times* (Nov. 26, 2020), <https://www.nytimes.com/2020/11/26/us/un-panel-technology-in-policing-can-reinforce-racial-bias.html?bgrp=a&smid=url-share> (on file with the *Columbia Law Review*) (last updated Dec. 7, 2020) (quoting Professor Rashida Richardson noting that “American police departments have fiercely resisted sharing details

Supreme Court has decided that the government's acquisition of cellphone location information requires a warrant,⁴² it has not addressed many questions about police departments' use of or access to other surveillance technologies. Many legal scholars have argued that the Fourth Amendment is ill suited to address the police technologies that have increased mass surveillance.⁴³ Some states have regulated specific technologies like the use of license plate readers,⁴⁴ and a small number of local governments have created administrative regulations for the use and purchase of surveillance technologies.⁴⁵ But there is no current comprehensive federal regulation on police departments' use of these technologies, nor on artificial intelligence more broadly.

II. EXPERIMENTATION AND BIOETHICS

This Part explains how the framework of experimentation offers an important and new understanding of how police use algorithmic surveillance technologies today. If we approach the use of these tools as experiments on communities, we can also then see why many of their uses have operated as poorly *designed*, *executed*, and *controlled* experiments. The framework of experimentation does not prohibit the use of algorithmic surveillance technologies but does demand that police justify, limit, and control the circumstances in which these experiments take place.

of the number or type of technologies they employ, and there is scarce regulation requiring any accountability for what or how they use them”).

42. See *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018) (holding that the government's acquisition of historical cell site information collected by a third party requires a warrant).

43. See, e.g., Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 Ala. L. Rev. 1, 8 (2022) (observing that “there is not a clear Fourth Amendment violation in [a] generalized mass surveillance state”); Wayne A. Logan, *Fourth Amendment Localism*, 93 Ind. L. Rev. 369, 383 (2018) (noting that the Supreme Court has “struggled, not altogether successfully, to craft doctrine amid rapidly changing technologies expanding police authority”).

44. See, e.g., *Automated License Plate Readers: State Statutes*, Nat'l Conf. State Legislatures, <https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes> [https://perma.cc/K2S3-SWKE] (last updated Feb. 3, 2022) (noting that “[a]t least 16 states have statutes that expressly address the use of ALPRs or the retention of data collected by ALPRs” (emphasis omitted)).

45. A 2020 study identified fourteen local governments that have passed formal controls over police surveillance technologies. Their most salient features include formal approval for acquisition and use, limits on contractual arrangements, and enforcement mechanisms. See Maily Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 Santa Clara High Tech. L.J. 481, 545–46 (2020).

A. *The Framework of Experimentation*

A central premise of research is adherence to the scientific method.⁴⁶ While there are variations in how different disciplines and institutions define the scientific method, they share some common features. Scientists engage in experimentation to advance knowledge in their field in ways that can be verified, refuted, or repeated. An experiment tests a falsifiable hypothesis about a phenomenon by gathering data according to set protocols.⁴⁷ The results of the experiment may refute or support that hypothesis and lead to a conclusion about the validity of that hypothesis.⁴⁸

We can borrow the term “experiment” from the scientific context because its emphasis on well-designed testing provides a helpful framework.⁴⁹ In the policing-technology context, experiments are unproven uses of an automated system by the police for surveillance and intervention on human subjects. Using a new algorithmic surveillance tool to decide if it “works” as promised—rather than apply an already-proven tool—means these tools operate as experiments. But because police do not apply the framework of experimentation, they fail to provide meaningful controls in the form of a hypothesis they have adopted, protocols they intend to follow, or metrics by which they will judge the success or failure of the experiment.

B. *Bioethics and Human Subjects*

Not only does the experimentation framework help us assess these new technologies, but these experiments also raise concerns because they are tested on *people and communities*. Special ethical considerations arise when conventional scientific experiments are conducted on human

46. See, e.g., 45 C.F.R. § 46.102(1) (2024) (defining research as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge”).

47. See, e.g., Off. of Rsch. Integrity, HHS, Module 1: Introduction: What Is Research?, <https://ori.hhs.gov/module-1-introduction-what-research> [https://perma.cc/9ABL-XR4A] (last visited Sept. 13, 2024) [hereinafter Off. of Rsch. Integrity, What Is Research?] (“A hypothesis is an informed and educated prediction or explanation about something.”); see also Off. of Rsch. Integrity, HHS, Basic Research Concepts: Additional Sections, <https://ori.hhs.gov/basic-research-concepts-additional-sections-0> [https://perma.cc/5AX8-A4M9] (last visited Sept. 13, 2024) (defining protocols as the “research plan developed by the researcher that should be followed when carrying out the study”).

48. Off. of Rsch. Integrity, What Is Research?, *supra* note 47 (“Part of the research process involves testing the hypothesis, and then examining the results of these tests as they relate to both the hypothesis and the world around you. . . . [A hypothesis] tells the researcher which factors are important to study and how they might be related . . .”).

49. Of course, these are not strictly scientific experiments in the sense that the police do not engage in randomization to negate the effects of unrelated variables. See Off. of Rsch. Integrity, HHS, Module 3: Elements of Research, <https://ori.hhs.gov/module-3-elements-research> [https://perma.cc/E6BT-JN4M] (last visited Oct. 25, 2024) (“Among the most important elements to be considered are variables, associations, sampling, random selection, random assignment, and blinding.”).

subjects. In biomedical and behavioral research, experimentation on human subjects is subject to external oversight and review.⁵⁰ Federal law defines human subjects research as that involving “a living individual about whom an investigator . . . [o]btains information . . . through intervention or interaction with the individual, and uses, studies, or analyzes the information.”⁵¹

The protection of human research subjects in the United States relies on principles heavily influenced by the 1979 report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, better known today as the Belmont Report.⁵² The Report identifies three key values that should guide human experimentation: respect for persons, beneficence, and justice.⁵³

A respect for persons demands that “individuals should be treated as autonomous agents” whose “considered opinions and choices” are entitled to respect.⁵⁴ The value of beneficence requires actions to secure the “well-being” of research subjects, including the maximization of possible benefits and the minimization of possible harms to those persons.⁵⁵ Finally, the principle of justice identified in the report emphasizes that injustice happens when “some benefit to which a person is entitled is denied without good reason or when some burden is imposed unduly.”⁵⁶ In the policing context, that balancing might weigh foreseeable material harms against improvements in policing, such as reductions in crime or improvements in clearance rates.

The Belmont Report takes note of heightened ethical concerns that arise in the very selection of which persons and communities are targeted for experimentation: Injustice can arise in the very selection of subjects for experimentation, leading to the unequal distribution of research benefits

50. Federally funded research must follow federal regulations regarding human subjects, including informed consent procedures. This requirement is in the Federal Policy for the Protection of Human Subjects, which is also referred to as the “Common Rule” and can be found in the HHS regulations at 45 C.F.R. § 46. First published in 1991, the Common Rule was updated in 2018. See Jerry Menikoff, Julie Kaneshiro & Ivor Pritchard, *The Common Rule*, Updated, 376 *New Eng. J. Med.* 613, 613 (2017) (describing the process of the first update to the Common Rule since its 1991 issue).

51. 45 C.F.R. § 46.102(e)(1) (2024).

52. Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, 44 *Fed. Reg.* 23,193 (Apr. 18, 1979) [hereinafter *Belmont Report*] (describing the “basic ethical principles” of research involving human subjects); see also Eli Y. Adahsi, LeRoy B. Walters & Jerry A. Menikoff, *The Belmont Report at 40: Reckoning With Time*, 108 *Am. J. Pub. Health* 1345, 1345 (2018) (describing the “watershed moment” that was the adoption of the Belmont Report).

53. Belmont Report, *supra* note 52, at 23,193.

54. *Id.*

55. *Id.* at 23,194.

56. *Id.*

and burdens in society.⁵⁷ Unethical treatment of persons and communities targeted by experimentation can lead to “unjust social patterns” in the “distribution of the burdens and benefits of research.”⁵⁸ Application of the experimentation framework to algorithmic surveillance tools should prompt the same concerns: whether these technologies are being used against vulnerable or underserved communities,⁵⁹ particularly in the context of discriminatory or disproportionate policing. When used in vulnerable or underserved communities, police technology experiments should pay attention to the balance of demonstrable benefits versus the minimization of harms.

The framing of experimentation is not far-fetched in the police technology context. It has already been proposed as a limiting consideration in the use of artificial intelligence. In its 2022 Blueprint for an AI Bill of Rights, the White House Office of Science and Technology Policy (OSTP) identified five core principles for the responsible use of artificial intelligence: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human alternatives.⁶⁰ The White House Blueprint defines the principle of data privacy as protection from “abusive data practices via built-in protections” and “agency” over how personal data is used.⁶¹ Some uses of AI, including health, education, and criminal justice, should be considered especially “sensitive” given the “intimate” nature of the data, the inability of individuals to “opt out,” and “historical discrimination that has often accompanied data knowledge.”⁶² In particular, the Blueprint refers to the need to protect the interests of *communities* as well as individuals.⁶³

Most importantly, the White House Blueprint warns that some types of personal information should be considered so “sensitive” that “novel uses” of AI may count as “human subject experimentation”—the same designation used for biomedical and behavior research.⁶⁴ Uses of AI that fall into these categories, which include instances in which “the algorithm

57. *Id.* at 23,196 (“Injustice may appear in the selection of subjects This injustice arises from social, racial, sexual and cultural biases institutionalized in society. Thus, . . . unjust social patterns may nevertheless appear in the overall distribution of the burdens and benefits of research.”).

58. *Id.*

59. By “underserved communities,” this Piece refers to “communities that have been systematically denied a full opportunity to participate in aspects of economic, social, and civic life.” See Off. of Sci. & Tech. Pol’y, *Blueprint for an AI Bill of Rights 11* (2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf> [<https://perma.cc/24XS-CNSB>] [hereinafter *AI Blueprint*].

60. *Id.* at 5–7.

61. *Id.* at 6.

62. *Id.* at 36.

63. See *id.* at 18 (“Identified risks should . . . include those to impacted communities that may not be direct users of the automated system, risks resulting from purposeful misuse of the system, and other concerns identified via the consultation process.”).

64. *Id.* at 38.

is dynamically developing and where the science behind the use case is not well established,” may require heightened review by “organizational compliance bodies” that apply “ethics rules and governance procedures.”⁶⁵

III. APPLYING THE EXPERIMENTATION FRAMEWORK

How does the approach of experimentation change our perspectives on how police adopt algorithmic surveillance technologies? This section examines three recent examples when local police departments adopted new technologies that later drew intense criticism. By evaluating these tools as experiments, we can (1) recognize their harms on the communities affected in ways that have not been adequately captured and (2) identify whether these tools worked, or whether they should have been adopted at all.

A. *Experiment One: Chicago’s Gun Violence Initiative*

One of the most alluring promises of the new surveillance tools is the capacity to predict risk: Who will engage in high-risk behavior that warrants intervention before it happens? Should a prediction tool forecast such information correctly, the police could save lives and reduce harms: a worthy project. But implemented as a poorly controlled experiment, such a tool might not just fail to predict risk but could also cascade into other secondary harms on the community.

The Chicago Police Department’s (CPD) experiment with its Strategic Subject List (SSL) provides one such example.⁶⁶ From 2012 to 2019, the Department used a risk assessment model to identify those most at risk for being either a perpetrator or victim of gun violence (“Party to Violence”) within the next eighteen months.⁶⁷ Every single person arrested in Chicago at least once during a four-year time period received a risk score of one to five hundred, which the CPD used to produce a rank-order list of those with the greatest risk.⁶⁸ The model factored in attributes including whether the person was a shooting victim, age at latest arrest,

65. *Id.* Notably, although the Blueprint’s discussion of “sensitive data” contexts includes “criminal justice,” OSTP chose not to discuss in any detail what that might mean for specific contexts including policing. See *id.* at 11. No explanation is given.

66. Off. of Inspector Gen., City of Chi., Advisory Concerning the Chicago Police Department’s Predictive Risk Models 1 (2020), <https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models.pdf> [<https://perma.cc/UAR9-MR8U>] [hereinafter *OIG Report*].

67. *Id.* at 1.

68. See *id.* at 2; see also Jeff Asher & Rob Arthur, Inside the Algorithm that Tries to Predict Gun Violence in Chicago, *N.Y. Times* (June 13, 2017), <https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html> (on file with the *Columbia Law Review*) (noting risk scores “range from 0 to 500, with higher scores representing increasing risk”).

and narcotics arrests (not convictions).⁶⁹ Those receiving the highest scores were said to be on the “heat list.”⁷⁰

Membership on the heat list led to practical consequences. The Chicago Police used these scores to guide decisionmaking, including which people would receive “custom notifications”: in-person visits at the homes of people identified as high risk by the model.⁷¹ During the visit, a CPD police officer would deliver a letter describing the information known to the police about the person’s criminal past, as well as a warning about consequences for future violent behavior.⁷² These were not stops or arrests based on any past criminal behavior but warnings about potential future violent behavior or victimization based on the risk model.⁷³ In theory, social services were supposed to be offered along with the police warnings in these visits.⁷⁴ Data released in response to a 2016 records request, however, showed that far more people with high scores were arrested than were offered social services.⁷⁵ In addition, those who received a custom notification may have received harsher charging decisions if later arrested.⁷⁶

A report by the Chicago Office of the Inspector General found the police department’s use of the SSL riddled with concerns.⁷⁷ The risk scores and tiers at the core of the program used for interventions were “unreliable”: The quality of its data was “poor” and the risk scores were

69. *Id.* at 1–2.

70. John Eligon & Timothy Williams, *Police Program Aims to Pinpoint Those Most Likely to Commit Crimes*, N.Y. Times (Sept. 24, 2015), <https://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html> (on file with the *Columbia Law Review*) (referring to the development of Chicago’s “heat list”).

71. OIG Report, *supra* note 66, at 2–3; Chicago Police Use “Heat List” as Strategy to Prevent Violence, Chi. Trib. (Aug. 21, 2013), <https://www.chicagotribune.com/2013/08/21/chicago-police-use-heat-list-as-strategy-to-prevent-violence/> [<https://perma.cc/3BSM-EE8A>] [hereinafter Chicago Police Heat List] (last updated Aug. 24, 2021) (describing personal visits from police “letters warning those on the heat list of the consequences of continued criminal behavior”).

72. Chicago Police Heat List, *supra* note 71. Custom notification visits were intended as opportunities to offer services but may have been sometimes little more than “going door-to-door notifying potential criminals not to commit any violent crimes.” Adrienne Balow & Judy Wang, CPD Launches New “Custom Notifications” Anti-Violence Program, WGN9 (July 19, 2013), <https://wgntv.com/news/cpd-launches-new-custom-notifications-anti-violence-program/> (on file with the *Columbia Law Review*).

73. See Balow & Wang, *supra* note 72 (“[T]he department narrowed the list to more than 400 ‘hot people’ who are most likely to commit shootings or become victims.”).

74. OIG Report, *supra* note 66, at 2–3.

75. Yana Kunichoff & Patrick Sier, *The Contradictions of Chicago Police’s Secretive List*, Chi. Mag. (Aug. 21, 2017), <https://www.chicagomag.com/city-life/august-2017/chicago-police-strategic-subject-list/> [<https://perma.cc/4SUR-7Z7N>] (explaining that twenty-six SSL-scored people attended a social services call-in while 280 SSL-scored people were arrested in 2016).

76. OIG Report, *supra* note 66, at 7.

77. See *id.* at 4.

not updated regularly.⁷⁸ And because the assessments relied in part on arrests—rather than convictions—the custom notification visits may have “resulted in interventions which effectively punished individuals for criminal acts for which they had not been convicted.”⁷⁹ Because the algorithm did not distinguish between arrests and convictions, that meant that someone could receive a high risk score—along with its attendant real-life consequences—even if the arrest had resulted in no charges or an acquittal.⁸⁰ Specifically, a person who received a custom notification as a result of an arrest-based high score “may have been subject to harsher charging decisions on subsequent arrests.”⁸¹

Additionally, because the Chicago police lacked “proper training or guidance” about how to use the risk scores, police officers may have misunderstood their meaning and thus their value in everyday policing.⁸² In its response to the report, the Chicago Police Department acknowledged its program as “experimental research” in predicting gun violence risks and suggested it might revisit other predictive models in the future.⁸³

The experimentation framework provides clarity as to why the SSL was flawed from its outset. What was the working hypothesis behind the experiment? Perhaps the hypothesis of the SSL was that early police intervention of policing resources for those identified as at high risk of gun violence or victimization would lead to measurably reduced gun violence compared to other policing approaches. A review of the Department’s 2013 pilot SSL program concluded that it “does not appear to have been successful in reducing gun violence.”⁸⁴ Despite this initial

78. *Id.* at 5 (noting that CPD data “retained risk scores . . . for individuals who were not arrested again within the four years” following initial calculation and “did not assess the risks of individuals . . . arrested after the risk scores . . . were last calculated” or “account for additional activity that could impact . . . risk scores and tiers”).

79. *Id.* at 7.

80. *Id.* at 7–8.

81. *Id.* at 7.

82. *Id.* at 5–6.

83. Email from Dana O’Malley, Gen. Couns., Off. of the Superintendent, Chi. Police Dep’t, to Joseph M. Ferguson, Off. of the Inspector Gen., City of Chi., CPD’s Response to OIG Advisory Concerning Predictive Risk Models (Jan. 7, 2020), <http://igchicago.org/wp-content/uploads/2020/01/CPD-Response-to-OIG-Advisory-on-Predictive-Risk-Models.pdf> [<https://perma.cc/DKR5-WE5K>].

84. Jessica Saunders, Priscillia Hunt & John S. Hollywood, Predictions Put Into Practice: A Quasi-Experimental Evaluation of Chicago’s Predictive Policing Pilot, 12 *J. Experimental Criminology* 347, 366 (2016). The study did, however, note that the pilot “may have improved justice by identifying more perpetrators.” *Id.* Rand researchers could not conclusively assess the reasons for this, although it appeared that “the impact of the SSL was on clearing shootings, but not on gun violence in general, during the observation window.” *Id.* at 365.

finding, the Chicago Police stopped evaluating its updated risk models over the next four versions of the SSL.⁸⁵

Proper protocols were neither carefully designed nor followed. The police used data inconsistently and haphazardly.⁸⁶ The very data underlying risk assessments “were not updated regularly.”⁸⁷ The resulting interventions were similarly flawed.⁸⁸ If Custom Notification Visits—including the offer of social services—were part of the experiment’s protocols, then these were never followed consistently.⁸⁹ In fact, the variability of approaches appears to have been intentional: District commanders could choose which actions to take.⁹⁰ That same lack of clarity about appropriate interventions to take against those identified on the “heat list” also meant that collateral harms were easily identifiable from the beginning.⁹¹ Without clear guidelines on appropriate police responses, police were free to intensify surveillance and scrutiny on persons not known to be engaged in criminal activity.

Finally, a years-long experiment resulting in heightened police interventions and surveillance of primarily young men of color ought to have considered ethical evaluations. How would an unproven set of potentially coercive interventions minimize harms and maximize benefits to the community policed? No such considerations existed with the SSL during its seven-year implementation period.

B. *Experiment Two: Chicago’s Gunshot Detection*

Artificial intelligence promises us the ability to make sense of the immense amount of data that we lack the human resources to process efficiently. In urban areas with high rates of gun violence, swift police response is a problem.⁹² Not every gunshot results in a call for service, and

85. OIG Report, *supra* note 66, at 8 (“Neither CPD nor RAND (which was periodically tasked with evaluating CPD’s PTV risk models) evaluated Versions 2 through 5 of the models.”).

86. *Cf. id.* at 6 (“Without proper training or guidance, district commanders may not have understood the purpose of PTV predictive models or how to apply risk scores or tiers . . .”).

87. *Id.* at 5.

88. *Cf. Saunders et al.*, *supra* note 84, at 355 (“Commanders were not given specific guidance on what treatments to apply to their SSL members . . .”).

89. *Cf. Kunichoff & Sier*, *supra* note 75 (noting that in 2016, of 1,024 attempted custom notifications attempted, only twenty-six involved meetings in which police, social workers, and others offered participants social services).

90. See *Saunders et al.*, *supra* note 84, at 355 (“The main guidance provided by central leadership was to use the programs detailed in Chicago’s Gang Reduction Strategies on SSL members when possible, but commanders were left wide discretion as to what actions their units should take.” (cleaned up)).

91. See *id.*

92. *Cf. C.R. Div. & U.S. Att’y’s Off., N. Dist. Ill., DOJ*, Investigation of the Chicago Police Department 140 (2017), https://www.justice.gov/d9/chicago_police_department_findings.pdf [<https://perma.cc/E2R6-2QK9>] [hereinafter DOJ, Chicago Police

relying on calls for service can lead to delays in response times.⁹³ An automated method of detecting gunshots could deliver faster police responses, increased apprehension of suspects, and eventually lower gun violence rates.⁹⁴ Yet a faulty tool might not only waste police resources but also increase police officers being primed to encounter gun violence and produce some unexpected consequences.

Chicago's experiment with acoustic gunshot technology provides such an example. In 2018, the Chicago Police Department entered into a three-year, \$33,000,000 contract with the acoustic gunshot detection vendor ShotSpotter (now SoundThinking⁹⁵).⁹⁶ The company's system purports to identify gunshots by picking up sounds captured by acoustic sensors placed on urban sites like buildings and street lights.⁹⁷ The company's proprietary algorithm filters the sounds picked up by the sensor and then identifies which sounds are likely gunshots.⁹⁸ ShotSpotter's analysts then check the audio files flagged by the algorithm to decide whether to alert their police department customers.⁹⁹ The technology is designed to assist police efforts by allowing them to send officers to precise places where gunshots—presumed to be a sign of gun violence—have been detected.¹⁰⁰ A working hypothesis for the city's experiment could

Department Investigation] (“Many residents in predominantly black or Latino areas complained about response times when they call the police for assistance.”).

93. Cf. Mitchell L. Doucette, Christa Green, Jennifer Necci Dineen, David Shapiro & Kerri M. Raissian, *Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties: A Longitudinal Analysis, 1999–2016*, 98 *J. Urb. Health* 609, 610 (2021) (“One of the major barriers in reducing urban firearm violence is the significant underreporting of shots fired.” (citation omitted)).

94. See *id.* (noting that the scholarly “literature demonstrates that ShotSpotter is a powerful surveillance tool with potential for assisting” the police).

95. Press Release, SoundThinking, *Shotspotter Changes Corporate Name to Soundthinking and Launches Safetysmart Platform for Safer Neighborhoods* (Apr. 10, 2023), <https://www.soundthinking.com/press-releases/shotspotter-changes-corporate-name-to-soundthinking-and-launches-safetysmart-platform-for-safer-neighborhoods/> [<https://perma.cc/82WV-8DSA>].

96. See Joseph M. Ferguson & Deborah Witzburg, *City of Chi. Off. of Inspector Gen., File No. #21-0707, The Chicago Police Department's Use of ShotSpotter Technology 2* (2021), <https://igchicago.org/wp-content/uploads/2021/08/Chicago-Police-Departments-Use-of-ShotSpotter-Technology.pdf> [<https://perma.cc/55GR-3UW2>] [hereinafter *OIG ShotSpotter*]. Because the contemporary reporting refers to the company as Shotspotter, this Piece will refer to the vendor by its previous name for ease of reference.

97. Garance Burke, Martha Mendoza, Juliet Linderman & Michael Tarm, *How AI-Powered Tech Landed Man in Jail With Scant Evidence*, Associated Press (Mar. 5, 2022), <https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220> [<https://perma.cc/9L7M-5XQD>].

98. The technology uses both triangulation and multilateration to approximate the location of a possible gunshot. See *OIG ShotSpotter*, *supra* note 96, at 4.

99. Garance Burke & Michael Tarm, *Confidential Document Reveals Key Human Role in Gunshot Tech*, Associated Press (Jan. 20, 2023), <https://apnews.com/article/shotspotter-artificial-intelligence-investigation-9cb47bbfb565dc3ef110f92ac7f83862> [<https://perma.cc/2K5G-BC3R>].

100. Doucette et al., *supra* note 93, at 610.

have been stated like this: Relying on automated gunshot detection to direct police responses will reduce gun violence.

In practice, however, Chicago's experiment with ShotSpotter did not lead to results consistent with that hypothesis. In a 2021 report, the Chicago Office of the Inspector General concluded that police responses to ShotSpotter alerts "*rarely produce* documented evidence of a gun-related crime, investigatory stop, or recovery of a firearm."¹⁰¹ While the Chicago police provided a response to each of the 50,176 probable gunshots detected by ShotSpotter between January 2020 and May 2021, only 9.1% of police responses resulted in discovery of evidence related to a gun offense, and only 2.1% resulted in an investigatory stop related to a possible gun-related offense.¹⁰²

Nor were ethical considerations part of the experiment's design. Sending in police officers primed to look for gun violence increases the possibility of violent interactions.¹⁰³ Police officers might incorrectly perceive a dangerous situation when, in fact, one is not present.

Indeed, ShotSpotter did change police perception and behavior in unexpected ways.¹⁰⁴ A Chicago police officer who conducts a *Terry* stop must complete an Investigatory Stop Report, which provides the facts supporting the officer's belief that the legally required reasonable suspicion for the stop exists.¹⁰⁵ In its sample review of Investigatory Stop Reports, the Chicago Office of the Inspector General discovered that some officers informally knew of areas with frequent ShotSpotter alerts; they would use this knowledge as a reason to conduct an investigative stop or to conduct a frisk of a person found there, even if the officer was not responding to a specific ShotSpotter alert.¹⁰⁶ In other words, the mere

101. OIG ShotSpotter, *supra* note 96, at 3 (emphasis added).

102. *Id.* at 2–3.

103. Brief of Chicago Community-Based Organizations Brighton Park Neighborhood Council et al. as Amici Curiae Supporting Respondent at 16, *Illinois v. Williams*, No. 20 CR 08996901 (Ill. Cir. Ct. 2021), <https://datafordefenders.org/wp-content/uploads/2023/03/Shotspotter-MacArthur-Amici-Brief-with-Footnotes.pdf> [<https://perma.cc/3D92-BL28>] (“Individuals in the vicinity of an alert are immediately under suspicion by officers who are primed to believe that they are entering a dangerous situation.”) [hereinafter MacArthur Report].

104. See Elizabeth Joh, *The Unexpected Consequences of Automation in Policing*, 75 S.M.U. L. Rev. 507, 523 (2022) [hereinafter Joh, *Consequences of Automation*] (highlighting that “some police officers justified stop and frisks not because they were responding to a specific alert, but because they were in an area they believed to be the site of previous alerts”).

105. Chi. Police Dep't, Special Order S04-13-09 IILC at 3 (July 10, 2017), https://www.aclu-il.org/sites/default/files/field_documents/exhibit_2b_-_special_order_s04-13-09_-_july_2017.pdf [<https://perma.cc/TZV4-6T9J>] (“Sworn members who conduct an Investigatory Stop are required to complete an Investigatory Stop Report.”).

106. OIG ShotSpotter, *supra* note 96, at 19, 22 (“OIG also identified 10 ISRs (13.9%) in which reporting officers referred to the *aggregate results of the ShotSpotter system* as informing their decision to initiate a stop or their course of action during the stop, even when they were not responding to a specific ShotSpotter alert.”).

existence of an automated system that generated alerts gave police cause to believe they were in a more dangerous situation that warranted stops and frisks they might otherwise not have conducted.¹⁰⁷

The experimentation framework also helps clarify what results should count. Directing police to areas because of an algorithmically detected gunshot results in more opportunities for those officers to engage in discretionary policing unrelated to gun violence.¹⁰⁸ A police officer who arrives at a city block looking for gun violence and finds none can often find other reasons to engage in investigative detentions or consensual encounters that would have not happened without the technological prompting.¹⁰⁹ Should we count an arrest for drug possession because an officer was directed to that place by an automated gunshot alert as evidence of the tool's success?¹¹⁰ The experimentation framework provides an easy response: No. We should not consider arrests under these conditions a measure of the experiment's success: These arrests prove nothing about the original hypothesis, had one been formalized.

The racial composition of the communities most affected by Chicago's gunshot-detection experiment also should have triggered ethical considerations about minimizing harm. A 2021 study of Chicago's ShotSpotter use by the MacArthur Justice Center found that the gunshot-detection system was deployed in the twelve city districts with the city's highest proportion of Black and Hispanic residents.¹¹¹ The tool was used in every district whose Black or Hispanic population was above sixty-five percent.¹¹² Not only did the MacArthur Justice Center conclude, like the Inspector General, that the vast majority of ShotSpotter alerts were unfounded, it also found that the presence of ShotSpotter in certain police districts and not others resulted in tens of thousands of excessive, unsubstantiated police deployments compared to districts where the technology was not in use.¹¹³ By contrast, unfounded police responses based on 911 calls were similar across all city districts.¹¹⁴ In the Center's view, the technology "exacerbates the systemic patterns of racialized policing and overpolicing" in the city.¹¹⁵

107. See Joh, *Undue Influence*, *supra* note 39, at 44.

108. Joh, *Consequences of Automation*, *supra* note 104, at 528.

109. Of the more than forty-six thousand ShotSpotter-initiated police contacts analyzed between July 2019 and April 2021, the MacArthur Justice Center found that the vast majority did not result in any incident involving a firearm, nor the discovery of any evidence of crime at all. Most were "incidents where police respond to a ShotSpotter alert but end up stumbling upon some other reportable incident." MacArthur Report, *supra* note 103, at 10.

110. See, e.g., *id.* at 10 (describing an example of such police conduct).

111. *Id.* at 13–14.

112. *Id.* at 14.

113. *Id.* at 14–16.

114. *Id.* at 14–16.

115. *Id.* at 16.

Finally, the experimental framework would have led to a clear conclusion for the city of Chicago. As the city's Inspector General found, the data did not bear out the implied hypothesis of the experiment: This particular algorithmic surveillance technology did not effectively address gun violence. That conclusion ought to have shelved the project, even apart from its lack of ethical constraints. Instead, in August 2021, the city renewed its three-year \$33,000,000 contract.¹¹⁶

C. *Experiment Three: Risk Prediction in Los Angeles*

Another promise of artificial intelligence is that it will improve the administration of criminal law by increasing objectivity and reducing problems of human bias in decisionmaking.¹¹⁷ An algorithmic surveillance technology that predicts high-risk individuals for police attention could provide a data-driven method of policing that would address historical problems with biased discretionary decisionmaking. But without careful design, protocols, or controls, such a tool could easily end up mirroring old problems instead of addressing them.

We can consider the LASER program implemented by the Los Angeles Police Department as the kind of police technology experiment that failed to reduce bias. Initially funded by the federal Smart Policing Initiative, Operation LASER (Los Angeles Strategic Extraction and Restoration) was first implemented in 2011 and ran until 2019.¹¹⁸ The program's explicit goal was to reduce violent and gun-related crime

116. CBS 2 Investigation: CPD Extends ShotSpotter Contract With No Public Notice, CBS News (Aug. 11, 2021), <https://www.cbsnews.com/chicago/news/cbs2-investigators-shotspotter-contract-extended/> [<https://perma.cc/UZ85-GVGB>] (noting that the contract was extended for an additional two years to August 2023 despite controversy). The subsequent administration of Mayor Brandon Johnson also renewed the contract. See Megan Hickey, Despite Promise Not to, Chicago's Mayor Extends ShotSpotter Contract for More Than \$10M, CBS News (June 15, 2023), <https://www.cbsnews.com/chicago/news/shotspotter-contract-renewal-10m/> [<https://perma.cc/8HMS-WVYV>]. Hours after the extended contract expired in September of 2024, the city announced it would explore other options for "first responder technology." A spokesperson for the Mayor's office stated that the city had spent more than fifty-three million dollars on ShotSpotter technology. See 'ShotSpotter,' Chicago's Gunshot Detection Technology System, Dismantled as Contract Expires, NBC Chi. (Sept. 23, 2024), <https://www.nbcchicago.com/news/local/shotspotter-chicago-gunshot-detection-technology-system-dismantled-as-contract-expires/3554765/> [<https://perma.cc/P9H5-8FMT>].

117. See Brayne, *supra* note 9, at 982 (noting that "part of the appeal of big data lies in its promise of less discretionary and more objective decision-making"); Jessica Eaglin, Racializing Algorithms, 111 Calif. L. Rev. 753, 756 (2023) (discussing how some scholars believe algorithms decrease individual bias and increase objectivity).

118. Off. of Inspector Gen., Review of Selected Los Angeles Police Department Data-Driven Policing Strategies 3–4 (2019), https://www.oig.lacity.org/_files/ugd/b2dd23_21f6fe20f1b84c179abf440d4c049219.pdf [<https://perma.cc/EM8N-7PSQ>] [hereinafter *OIG Laser*]; Mark Puente, LAPD Ends Another Data-Driven Crime Program Touted to Target Violent Offenders, L.A. Times (Apr. 12, 2019), <https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html> (on file with the *Columbia Law Review*).

through prediction—identifying persons and places that warranted extra police attention.¹¹⁹ Relying explicitly on a medical analogy, Operation LASER was designed like “laser surgery” to target “violent repeat offenders” who “commit crimes in the specific target areas.”¹²⁰ The program would help police act in the same way “a trained medical doctor uses modern technology to remove tumors” by “diagnos[ing]” problematic persons and places.¹²¹ Thus, the working hypothesis: Objectively data-driven predictions about high-risk individuals would reduce violent and gun-related crime.

Operation LASER created Crime Intelligence Details (CID), teams of officers and crime analysts working to gather information and create lists of “chronic offenders.”¹²² These individuals were first selected on the basis of arrest reports, investigative reports, and field interview cards produced daily during ordinary patrols to find “anything related to violent crime [or] incidents that involved a gun.”¹²³ The CIDs would then develop a “work-up” of each selected person with the use of Palantir systems.¹²⁴ Palantir, a private technology company, provides a platform to law enforcement agencies like the LAPD that assembles many types of data—including not just traditional criminal histories but also noncriminal data, such as repossession and collection agency information, retail purchases, and utility bills—to link seemingly unconnected data to build intelligence and help assemble a profile.¹²⁵

Each person selected for a work-up was given a point total based on their criminal history and the following factors: five points for being a gang member, five points for being on parole or probation, five points for any prior arrests with a handgun, five points for any violent crimes on a rap sheet, and one point for every “quality police contact” in the last two

119. *OIG Laser*, supra note 118, at 4.

120. *Id.* (internal quotation marks omitted) (quoting Craig D. Uchida et. al., *The Los Angeles Smart Policing Initiative: Reducing Gun-Related Violence Through Operation LASER 6* (2012), <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/losangelesspi.pdf> [<https://perma.cc/97XX-4J3P>]).

121. *Id.* (internal quotation marks omitted) (quoting Craig D. Uchida et. al., *The Los Angeles Smart Policing Initiative: Reducing Gun-Related Violence Through Operation LASER 6* (2012), <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/losangelesspi.pdf> [<https://perma.cc/97XX-4J3P>]).

122. *Id.* at 5.

123. *Id.* at 5. A field interview card contains information including name, address, physical features, vehicle information, gang affiliations, and criminal history, as well as a blank space for officers to add additional detail discovered during the stop. *Brayne*, supra note 9, at 998.

124. *Brayne*, supra note 9, at 994.

125. Mark Harris, *How Peter Thiel’s Secretive Data Company Pushed Into Policing*, *Wired* (Aug. 9, 2017), <https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/> (on file with the *Columbia Law Review*); see also *Brayne*, supra note 9, at 987 (explaining the relationship between these technologies and police communications).

years.”¹²⁶ Each geographic area using the LASER program was instructed to maintain a list of at least twelve of the high-scoring Chronic Offenders at all times, plus other persons to serve as potential replacements.¹²⁷ The commanding officer for each area was tasked with assigning personnel to each Chronic Offender for follow-up interventions, including sending letters to the person, conducting “door knocks” to advise of available services, and conducting warrant and parole or probation checks.¹²⁸ The promise of these tools was a more objective basis to identify risk and to direct police intervention.¹²⁹

In its review of the program, the Los Angeles Inspector General found that LASER fell far short of a precise, scientific approach to assessing and predicting criminal risks. There were systemic problems with the experiment’s design, oversight, and administration.¹³⁰ Its review found that LASER harbored “significant inconsistencies” in the program’s administration, lacked “formalized and detailed protocols and procedures,” and its data was collected in a way that made it “difficult” to determine whether the program had any significant impact.¹³¹ Not only was data collection unreliable and implementation across districts inconsistent, but the very working hypothesis of LASER changed over time.¹³² This lack of “clarity [of] the overall goal of the program itself” also made it nearly impossible for the Inspector General to evaluate whether the program was successful in its goals, as its goals did not remain consistent.¹³³

One aspect of the LASER experiment undermines a central premise of algorithmic surveillance technology: that it introduces objectivity and thereby reduces human bias. A carefully designed experiment should provide clear protocols to minimize the introduction of human bias and error. Despite its reliance on terms like “known risk factors” and “pre-determined criteria,” which help convey scientific precision and avoid

126. OIG Laser, *supra* note 118, at 6. In 2017, two criteria were modified to include five points “for each violent crime arrest” over the past two years, and five points “for each incident involving a gun over the last two years.” *Id.* at 6.

127. *Id.* at 5–6.

128. *Id.* at 7.

129. *Id.* at 3 (noting that LASER is a project federally funded to “replicat[e] evidence-based practices or to encourage exploration of new, unique solutions” (internal quotation marks omitted) (quoting Michael Medaris & Alissa Huntoon, BJA Fact Sheet, FS 000315, Smart Policing Initiative 1 (2009), https://www.ojp.gov/sites/g/files/xyckuh241/files/media/document/smart_policing_fact_sheet.pdf [<https://perma.cc/Q8EJ-CNMD>])).

130. *Id.* at 23–24 (noting that the “OIG identified significant barriers” in evaluating the program, including the lack of reliable data, variation in implementation, and lack of clear goal establishment).

131. *Id.* at 1.

132. *Id.* at 16.

133. *Id.* at 24.

discriminatory practices,¹³⁴ the LASER program contained significant opportunities for police officers to inject discretionary decisions into the predictive judgments at the core of its algorithmic tool.¹³⁵ The LASER program provided multiple opportunities for officers to manipulate results.¹³⁶

The problem was central to the selection of Chronic Offenders. Recall that LASER analysts would select people for “work ups”—a point total based on several factors, including one point for every “quality police contact” a person had in the last two years.¹³⁷ Officers understood that contacts could be based on information gleaned from investigative street stops and compiled into field interview “FI” (police contact) cards.¹³⁸ These might be *Terry* stops based on reasonable suspicion of a crime or consensual encounters in which the officer asks for a person to answer questions.¹³⁹ Under the Fourth Amendment, police may engage in *Terry* stops or consensual stops no matter their subjective motivation, so long as the underlying reasonable suspicion or voluntary consent can be established.¹⁴⁰

As Professor Sarah Brayne has reported in her study of the program, under LASER, police officers were incentivized to “get them in the system”: to obtain as many FIs from individuals as they could.¹⁴¹ One of the program’s creators admitted that “[m]ost of the time [the FI cards] didn’t lead to anything, but it was . . . data that went into the system, and that’s what [they] wanted.”¹⁴² Officers understood that they could influence the tally of quality police contact points by engaging in multiple stops of the same person: “I’m gonna give him two weeks and I’ll go FI him again. *It’s one point for every police contact.*”¹⁴³ These stops could be based on nonviolent minor offenses, like jaywalking, and even conducted with the

134. Craig D. Uchida et al., *The Los Angeles Smart Policing Initiative: Reducing Gun-Related Violence Through Operation LASER 7–8* (2012), <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/losangelesspi.pdf> [<https://perma.cc/97XX-4J3P>].

135. See supra text accompanying footnotes 130–135.

136. See Brayne, supra note 9, at 998 (discussing how officers create a “feedback loop” of point values).

137. OIG Laser, supra note 118, at 6.

138. Brayne, supra note 9, at 998.

139. *Terry v. Ohio*, 392 U.S. 1, 30 (1968) (holding that police may engage in brief investigatory searches and seizures when officer observes criminally suspicious activity and infers that person may be armed).

140. Cf. *Whren v. United States*, 517 U.S. 806, 813 (1996) (rejecting consideration of “actual motivations” of police officers in determining Fourth Amendment reasonableness of traffic stops).

141. Brayne, supra note 9, at 987 (internal quotation marks omitted) (quoting an LAPD captain).

142. Harris, supra note 125 (second alteration in original) (internal quotation marks omitted) (quoting Craig Uchida, a researcher in data-driven policing who shaped Los Angeles’s approach to predictive policing).

143. Brayne, supra note 9, at 987 (quoting an LAPD officer).

purpose of simply increasing quality police contact points.¹⁴⁴ Thus, this single aspect of LASER's prediction algorithm meant that police decisions to conduct stops or consensual encounters were "both causes and consequences of high point values."¹⁴⁵ Investigative stops could lead to recurring loops of discretionary policing yet also undergird LASER's predictive assessments.¹⁴⁶

Even the protocols around these data points were poorly defined and controlled. The program documents *did not define* what constituted qualifying police contact.¹⁴⁷ The program contained "significant inconsistencies" in how Chronic Offenders were selected, retained, surveilled, and tracked.¹⁴⁸ LASER documents also suggested incorrectly that officers could stop people simply because they had been designated as Chronic Offenders—stops that would have violated their Fourth Amendment rights.¹⁴⁹ Finally, officer training in implementing the LASER program appeared to be "informal," in many cases increasing further opportunities for irregular, discretionary, and unequal policing.¹⁵⁰

The LASER program embodied a police technology experiment flawed from its inception and in its execution. If the program's working hypothesis was that a predictive risk assessment would identify dangerous people for police intervention to reduce crime, the experiment suffered from poorly designed protocols, inconsistent data collection, and a lack of oversight. And as the Inspector General noted, the working hypothesis of the program changed in ways that made it difficult to evaluate success.¹⁵¹ Did LASER's results prove its thesis? The very flawed nature of the experiment meant that there were "significant barriers" to evaluating the program.¹⁵²

Moreover, the experiment's flawed design permitted collateral harms—the tolerance of highly discretionary police decisionmaking to support seemingly objective point tallies. Those persons targeted frequently for minor offenses like jaywalking simply because an officer

144. See *id.*

145. *Id.*

146. *Id.* at 998.

147. OIG Laser, *supra* note 118, at 6. The OIG report noted this although the conduct was informally explained to be a contact where "a gun was involved in the underlying incident." *Id.* at 6 & n.8.

148. *Id.* at 16.

149. *Id.* at 11 ("After suggesting that officers who see designated Chronic Offenders 'may stop them, do a field interview, and let them go, if appropriate,' the document also states that '[i]n many situations, however as with all stops, [the stops] should be constitutional and legal.'" (alteration in original) (quoting "documents provided" to OIG)).

150. *Id.* at 12.

151. *Id.* at 5, 24 (noting that one of the "primary areas that lacked clarity was the overall goal of the program itself," which "evolved over time" and thus rendered evaluation difficult).

152. *Id.* at 23.

sought LASER points were subjected to seemingly arbitrary policing. Such perceptions of unfairness undermine public perceptions of police legitimacy.¹⁵³ These were entirely foreseeable potential harms based on decades of police research that could have been designed into the LASER experiment but were not.

D. *Police Technology Experiments and Vulnerable Communities*

Not only did these three experiments suffer from poorly defined hypotheses, protocols, and implementation, but they also failed to consider that the potential risks and harms of the experiments would be borne disproportionately by communities historically underserved by their police. Here, the framework of experimentation on human subjects is useful because it demands ethical considerations before any experimentation begins.

Police experimentation with the Strategic Subject List and ShotSpotter cannot be extricated from the historical context of policing practices in low-income, minority neighborhoods in Chicago. A 2015 DOJ investigation of the Chicago Police Department found that many residents of the city's predominately Black and Hispanic communities "experience policing in a fundamentally different way" from white residents and communities in the same city.¹⁵⁴ These differences involved both underpolicing and overpolicing. Residents in these marginalized communities reported to investigators that they felt "disregarded" by the police department when reporting they had been victimized by crime.¹⁵⁵ At the same time, many residents of Chicago's predominantly Black and Hispanic neighborhoods reported to DOJ investigators police treatment "so demeaning [that] they felt dehumanized," and police behaviors that created the impression that the "CPD is an occupying force."¹⁵⁶ These communities experience the highest rates of violent crime in the city and thus face a greater degree of police contact.¹⁵⁷ But aggressive stops, "jump outs" by unmarked cars and plainclothes officers, verbally abusive behavior, and repeated instances of excessive force with racially disparate

153. See generally Jason Sunshine & Tom R. Tyler, *The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing*, 37 *Law & Soc'y Rev.* 513 (2003) (exploring the connection between public support and police legitimacy, as well as what drives police legitimacy).

154. DOJ, *Chicago Police Department Investigation*, supra note 92, at 139.

155. *Id.* at 140.

156. *Id.* at 143, 146.

157. Patrick Sharkey & Alisabeth Marsteller, *Neighborhood Inequality and Violence in Chicago, 1965–2020*, 89 *U. Chi. L. Rev.* 349, 361 (2022) ("Although the precise locations of the most extreme violence within [Chicago] have shifted over time, the maps reveal a set of neighborhoods in the South and West Sides of the city that have consistently been the most violent neighborhoods of Chicago.").

impacts have contributed to perceptions of low trust and weak legitimacy.¹⁵⁸

These are the same communities in which the Chicago Police Department experimented with algorithmic surveillance tools. The Department's "heat list" was compiled and guided police conduct for seven years.¹⁵⁹ The use of acoustic gunshot detection has continued with the city's repeated renewals of its ShotSpotter contract despite the concerns raised by the city's Office of the Inspector General and a class action lawsuit.¹⁶⁰

As with Chicago, police technology experiments in Los Angeles must also be understood in a broader historical context. The formal city review of the Los Angeles Police Department after the infamous 1991 police beating of Rodney King is illustrative of a department with a documented history of racially discriminatory policing. The report of the Independent Commission on the Los Angeles Police Department, also known as the Christopher Commission, found that a "significant" number of officers repetitively used excessive force.¹⁶¹ That excessive force was exacerbated by racist attitudes documented among police officers.¹⁶² The report observed that "[w]ithin the minority communities of Los Angeles," there existed "long-standing complaints" that officers treated racial minorities differently—and more harshly—than they did white residents.¹⁶³

This means that the failures, costs, and burdens of these technology experiments have been borne disproportionately by communities with persistent problems of excessive force, low trust, and policing tactics perceived as unfair. The use of these technological instruments in these particular communities are innovations from one perspective—but in practice, they have also imposed an unequal distribution of research benefits and burdens in society from an ethical point of view.

E. *Police Technology Experiments*

Police technology experiments are not inherently bad, but poorly designed ones that produce foreseeable and unjustifiable harms are. So too are experiments that continue to operate after they fail to deliver any

158. Sharkey & Marsteller, *supra* note 157, at 144 ("The impact of these widespread constitutional violations, combined with unaddressed abusive and racially discriminatory conduct, have undermined the legitimacy of CPD and police-community trust in these communities.").

159. OIG Report, *supra* note 66, at 1.

160. *Williams v. Chicago*, No. 1:22-cv-03773 (N.D. Ill.), <https://www.courtlistener.com/docket/63888183/williams-v-city-of-chicago/>; OIG ShotSpotter, *supra* note 96, at 22 (noting that, while ShotSpotter may offer benefits, the technology "rais[es] the specter of poorly informed decision-making by responding" officers).

161. *Indep. Comm'n on the L.A. Police Dep't, Report of the Independent Commission on the Los Angeles Police Department*, at iii (1991).

162. *Id.* at 70.

163. *Id.*

proof of success. When local law enforcement agencies want to try new algorithmic surveillance tools, they are testing out a tool on a community with public resources and in the public interest. Accordingly, we should expect the police to follow basic principles: clarity as to their objectives, methods, and evaluation; acknowledgment of ethical obligations, particularly with vulnerable communities; and whether some experiments should be undertaken at all.

At a minimum, police technology experiments should engage in pre-experiment review that includes whether testing on the community is justified in the first place, given the potential harms balanced against the promised benefits. The experiment itself should contain a clear testable hypothesis about the technology, defined means of implementing the experiment as well as collecting data for later evaluation. A police technology experiment considered worthy of adoption should undergo mandatory evaluation of whether its findings support its hypothesis, as well as whether unexpected collateral harms counsel against the use of the technology. Finally, no experiment deemed a failure should be permitted to continue.

Today's police technology experiments do not follow this model and operate with few restraints. Some experiments in large cities like Chicago and Los Angeles have undergone detailed assessment by third parties, but not every city maintains an Inspector General, and these oversight bodies are not tasked with evaluating every experiment. No police technology experiment should begin without a hypothesis, well-defined and reviewed protocols, and clear measures of the experiment's success or failure.

CONCLUSION

Although the increasing use of algorithmic surveillance tools in policing has drawn widespread attention, one important perspective has thus far been missing. The adoption of these tools by local law enforcement agencies function as unchecked technological experiments on human subjects. These are experiments because the efficacy of these tools is often unknown or theoretical, and yet their use can impose material consequences in communities. This Piece provides some insights into how these experiments have become an increasing feature of ordinary policing and discusses why unchecked experimentation poses a distinct issue worthy of serious attention apart from technical or Fourth Amendment critiques.

FIGURE 1. A FRAMEWORK FOR EVALUATING POLICE TECHNOLOGY EXPERIMENTATION

