# RECKLESS AUTOMATION IN POLICING

*Elizabeth E. Joh*[†]

## TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z380P0WR7H

[†] Professor of Law, U.C. Davis School of Law. Thanks to the members of the Berkeley Technology Law Journal for organizing the 2021 symposium, "Technology Law as a Vehicle for Anti-Racism."

## I. INTRODUCTION

Automated decision-making plays an increasingly larger role in policing.[1] Traditional methods of police investigation have been augmented by tools like facial recognition, predictive analytics, license plate readers, and robotics.[2] These tools allow the police to sift through large amounts of information at a scale and speed not practicable with human skills alone. This reliance on artificial intelligence, however, has prompted numerous questions about how to balance criminal investigation needs with concerns about fairness, bias, transparency, and accountability. These concerns aren't unique to policing. You can find similar calls for "algorithmic accountability" in healthcare, banking, credit scoring, public benefits, and employment.[3]

How should we evaluate the growth of automation in policing? There is no shortage of answers, but this Article starts with a simple observation: by focusing on automation's harms to persons first. American policing is rife with reckless automation. The highly decentralized system of policing in the United States, with its more than 18,000 agencies,[4] permits and encourages experimentation with new technologies. Innovation in policing can, of course, be positive. Crime control and public safety are complex and evolving social problems, and over time, the police change their tactics and tools to address them.

[1] A recent report on predictive policing summarized the current use of technology in policing this way: "As the cost of collecting, storing, and analyzing data falls to nearly zero, we should expect a proliferation of data analysis tools and algorithmic mediation between the citizen and the state." *See* ETHICS + EMERGING SCIENCES GROUP, ARTIFICIAL INTELLIGENCE + PREDICTIVE POLICING: AN ETHICAL ANALYSIS 23 (2020).

[2] *Cf.* Andrew G. Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1114 (2017) (noting that "the first generation of predictive policing technologies represents only the beginning of a fundamental transformation of how law enforcement prevents crime"). A partnership between the Electronic Frontier Foundation (EFF) and the University of Nevada, Reno Reynolds School of Journalism has produced the Atlas of Surveillance, an ongoing project that maps the use of law enforcement technologies like predictive policing, face recognition, and license plate readers. *See* EFF: ATLAS OF SURVEILLANCE, https://atlasofsurveillance.org/ [https://perma.cc/4PS2-FXVQ] (last visited Apr. 15, 2022).

[3] There is already a large literature on algorithmic accountability and transparency, with many different approaches. Some notable examples include: Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 20 (2014); Tal Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503 (2013); Devin R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1 (2017); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017).

[4] BUREAU OF JUST. STAT., NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 1 (2016) ("Law enforcement in the United States is made up of about 18,000 federal, state, county, and local agencies.").

But new technologies that rely on artificial intelligence and the vast amounts of digital information now available have introduced new problems.[5] Police departments have bought, licensed, adopted, and experimented with technologies that impact communities through increased but invisible surveillance, and with mistakes that impose real-life consequences in police-civilian interactions. And these technological experiments are often deployed in places or against communities that have already been overpoliced. Those who are disproportionately and frequently affected by these experiments are black, brown, low-income, and without significant political power. We should identify this development as reckless automation in policing.[6]

Reckless automation has tangible consequences: its mistakes lead to street stops, arrests, and traffic stops of individuals. Communities also experience the psychological costs of pervasive (and sometimes barely visible) automated surveillance. Sometimes these policing experiments are conducted without the knowledge of the communities involved.

If we accept the premise of reckless automation, the conversation about accountability, artificial intelligence, and policing might benefit from a seemingly unrelated policy framework: that of experimentation on human subjects. The comparison may seem far-fetched. Yet even the police may think of their new technologies in the same way that the medical community approaches experimentation. The Los Angeles Police Department, for instance, referred to amount of police time spent at a place identified by a predictive policing program as "dosage."[7] Borrowing from that framework does not imply that reckless automation in policing is the literal equivalent of medical or psychological experiments on human subjects. Nor does such a comparison imply that the technical aspects of institutional review boards

[5] *Cf.* DAVID G. ROBINSON & MIRANDA BOGEN, AUTOMATION AND THE QUANTIFIED SOCIETY 9 (2017) ("Governments around the world increasingly use automation to make important decisions about people's lives, often without broad consultation or careful assessment of new systems' impact.").

[6] "Reckless" here is used in the criminal law sense: the conscious disregard of a substantial and unjustifiable risk. *See* MODEL PENAL CODE § 2.02(2)(c) (AM. L. INST. 1985).

[7] In its 2019 review of the PredPol predictive policing software used by the L.A.P.D., the Los Angeles Inspector General noted that "the amount of time an officer spends in a PredPol hotspot is referred to as dosage, which can be measured in minutes or hours." OFF. OF THE INSPECTOR GEN., REVIEW OF SELECTED LOS ANGELES POLICE DEPARTMENT DATA-DRIVEN POLICING STRATEGIES 25 (2019). Ultimately, the review concluded that the effectiveness of PredPol based "dosage" was inconclusive. *Id.* at 29. In its highly critical review of the data-driven LASER program, the Inspector General noted the Department referred to it this way: "The program is analogous to laser surgery, where a trained medical doctor uses modern technology to remove tumors or improve eyesight." *Id.* at 4.

should apply directly to new policing strategies.[8] But turning to a bioethical framework has value because it draws attention to the *subjects*—the communities affected—of policing. To the extent that the ethical considerations applied in human subjects research provide useful insights to apply to the many changes in policing, they open a new conversation. What if we think of new forms of automated decision-making in policing as experiments on communities that might impose harms with life-altering decisions?[9]

## II. AUTOMATION AND ACCOUNTABILITY

We all know about the influence of artificial intelligence and automation in our lives, from the most mundane experiences, like picking favorite songs or movies, to more important decisions like who should receive job interviews or who should receive government benefits.[10] That automation is also a part of policing. License plate readers today use algorithms to quickly identify individual plates. Facial recognition technology can quickly identify faces in fixed databases or in real-time scans. Software identifies high-risk persons and places.

All of this automation falls under the umbrella of "artificial intelligence": the use of machines to assume cognitive tasks usually performed by people.[11] That is a very broad definition, and rightly so: artificial intelligence can involve everything from the application of straightforward algorithms[12] to more complicated examples of machine learning that adapts to identify patterns in data.[13] Some artificial intelligence simply provides more information for

[8] And, in fact, federal regulations on human subject research explicitly exclude data collected for "criminal investigative purposes." 45 C.F.R. § 46.101(*l*)(4).

[9] *Cf.* ROBINSON & BOGEN, *supra* note 5, at 14 (describing "life-altering" effects of automation).

[10] Artificial intelligence is an umbrella term for machines that perform cognitive tasks. One form of artificial intelligence, machine learning, involves programming computers to detect patterns in provided data. *See, e.g.*, Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 404 (2017).

[11] *See* ROBINSON & BOGEN, *supra* note 5, at 11.

[12] *See id.* at 14 ("[A]lgorithms are simply a sequence of steps used to accomplish some task.").

[13] While artificial intelligence (AI) has been researched since the 1940s, the importance and pervasiveness of AI today is a result of 1) the availability of huge amounts of data, 2) improvements in machine learning, and 3) improvements in computing power. *See* CONG. RSCH. SERV., ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 2 (2020).

human decisionmakers (risk assessments in finance[14]), while other forms perform the analysis and the action (hiring and employment decision-making).[15]

But automation also poses questions about bias, secrecy, unaccountability, and mistakes that are hard to spot when the decision originates from a machine and not a person.[16] While the United States lacks a comprehensive data protection regime, many regulatory approaches have been proposed and some have become law. These proposals can apply to automated decision-making generally, or to more specific subject matters like policing and criminal justice.

We can summarize some of the predominant approaches to ethics and accountability in artificial intelligence.

First, because machine learning involves the identification of patterns from enormous data sets, the constitution of that training data can be a problem.[17] If a dataset of faces has many more white people then non-white people, then a facial recognition program instructed to identify faces can misidentify those

[14] *See, e.g.*, ORG. FOR ECON. COOP. AND DEV., ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND BIG DATA IN FINANCE: OPPORTUNITIES, CHALLENGES AND IMPLICATIONS FOR POLICY MAKERS 29 (2021), https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf [https://perma.cc/7Q44-FGBF] ("AI-based models and big data are increasingly being used by banks and fintech lenders to assess the creditworthiness of prospective borrowers and make underwriting decisions.").

[15] *See, e.g.*, Spencer Soper, *Fired by Bot at Amazon: "It's You Against the Machine,"* BLOOMBERG (June 28, 2021), https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out [https://perma.cc/87Q3-25MS] ("At Amazon, machines are often the boss—hiring, rating[,] and firing millions of people with little or no human oversight.").

[16] *Cf.* Calo, *supra* note 10, at 407 (noting "AI presents unique and important ethical questions").

[17] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 680 (2016) (defining training data as "quite literally the data that train the model to behave in a certain way"); Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/25NH-J5YV] ("If the data used to train the algorithm are more representative of some groups of people than others, the predictions from the model may also be systematically worse for unrepresented or under-represented groups."); XAVIER FERRER, TOM VAN NUENEN, JOSE M. SUCH, MARK COTÉ & NATALIA CRIADO, BIAS AND DISCRIMINATION IN AI: A CROSS-DISCIPLINARY PERSPECTIVE 1 (2020), https://arxiv.org/pdf/2008.07309.pdf [https://perma.cc/AT9Y-XWBS] (noting "algorithms learn to make decisions or predictions based on datasets that often contain past decisions. If a dataset used for training purposes reflects existing prejudices, algorithms will very likely learn to make the same biased decisions.").

who are not white at much higher rates than whites.[18] One study of facial recognition algorithms found that that while white men were correctly identified nearly all the time, black women were incorrectly identified up to a third of the time.[19] Put simply, biased data will lead to biased results.[20] This concern has prompted both calls for better training data and for bans or pauses on the use of facial recognition technology until these problems have been addressed.[21]

Relatedly, there can be bias in the algorithms themselves. People create algorithms, and their assumptions about the appropriate design and execution of the algorithm may create further biases. A recruitment algorithm, for instance, that uses men as the model for professional "fit" will disadvantage female applicants.[22] Of course, bias is not a new idea. But in this context, bias—whether in training data or in the instructions themselves—can magnify inequalities by reproducing these effects on a very large scale. Some scholars have proposed as a solution public access both to source codes and data sets.[23]

Another proposal in artificial intelligence policy is the call for explainability. With some complex uses of artificial intelligence, programmers may not be able to explain exactly why or how particular outcomes have been achieved. This black box problem means that a person may not be able to know why a particular prediction or decision was made.[24] Thus, there have been calls for a "right to explanation" when, for example, a person receives an adverse employment decision through automation.[25] And although calling for

[18] Natasha Singer, *Amazon is Pushing Facial Technology that a Study Says Could Be Biased*, N.Y. TIMES (Jan. 24, 2019), https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html [https://perma.cc/DL4W-9L6F].

[19] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/4HZQ-3HKW].

[20] *See, e.g.*, Citron & Pasquale, *supra* note 3, at 4 ("Scoring systems mine datasets containing inaccurate and biased information provided by people.").

[21] *See, e.g.*, Turner Lee et al., *supra* note 17.

[22] *See id.*

[23] *See, e.g.*, Citron, *supra* note 3, at 1308; Citron & Pasquale, *supra* note 3, at 26 ("Ideally, the logics of predictive scoring systems should be open to public inspection.").

[24] *See, e.g.*, Jessica Newman, *Explainability Won't Save AI*, BROOKINGS (May 19, 2021), https://www.brookings.edu/techstream/explainability-wont-save-ai/ [https://perma.cc/QL5X-997N] ("Much of artificial intelligence . . . is plagued by the 'black box problem.' While we may know the inputs and outputs of a model, in many cases we do not know what happens in between.").

[25] The EU's General Data Protection Regulation (GDPR), for instance, provides for a "right to be informed" about algorithmic decision-making. For a comprehensive analysis of the GDPR right to explanation, see Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 209–17 (2019).

the explanation of why an automated process led to a person's rejection for a loan, a job, or benefits has appeal, there is not yet widespread consensus on what form that explainability should take.[26] The right to an explanation can be combined with other tools from a legal framework to provide individuals with "technological due process" rights in automated decision-making.[27]

Another critique of opacity in automated decision-making arises because these tools are often developed within the private sector.[28] Government entities, including law enforcement agencies, typically do not design or create these systems.[29] Instead, public agencies usually stand in a customer-vendor relationship with private companies and then adopt the tools of algorithmic decision-making as a matter of purchase, lease, or contract.[30] These relationships complicate accountability considerably. If a person receives an adverse decision for government benefits because of a prediction tool developed privately, the agency may be unable to provide an explanation for the reasoning because the vendor invokes its proprietary interests and refuses to provide information. Criminal defendants have encountered problems, for example, in trying to access the source code for the privately developed "probabilistic typing" software that has identified them as a suspect by analyzing DNA samples that are usually too difficult for traditional forensics labs to assess.[31]

These approaches to algorithmic accountability each identify important problems in the uses of automated decision-making. Each proposes solutions

[26] ROBINSON & BOGEN, *supra* note 5, at 15.

[27] Citron, *supra* note 3, at 1306 (arguing for a due process framework in automating decision-making, including the right of explanation).

[28] *See, e.g.,* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (arguing that trade secrets regarding criminal justice technologies should not be privileged in criminal proceedings).

[29] Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CAL. L. REV. 917 (2021) (noting new technologies of surveillance, often procured from or otherwise reliant on the private sector, tend to operate in opaque and unaccountable ways).

[30] *See, e.g.*, Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19 (2017), https://www.nyulawreview.org/online-features/the-undue-influence-of-surveillance-technology-companies-on-policing/ [https://perma.cc/4VLX-3LW6] (discussing influence of private companies producing surveillance hardware and software on democratic policing).

[31] *See, e.g.*, Lauren Kirchner, *Where Traditional DNA Testing Fails, Algorithms Take Over*, PROPUBLICA (Nov. 4, 2016), https://www.propublica.org/article/where-traditional-dna-testing-fails-algorithms-take-over [https://perma.cc/G729-9QPJ] ("Defendants' requests to get access to TrueAllele's source code have consistently been denied."). *But see, e.g.*, Lauren Kirchner, *Powerful DNA Software Used in Hundreds of Criminal Cases Faces New Scrutiny*, THE MARKUP (Mar. 9, 2021), https://themarkup.org/news/2021/03/09/powerful-dna-software-used-in-hundreds-of-criminal-cases-faces-new-scrutiny [https://perma.cc/YP8Q-A35F].

that can be implemented in new regulations and agency decision-making. And all have influenced efforts to regulate automated decision-making around the country. In policing, concerns about secrecy, for instance, have led some local governments to impose notice and reporting requirements on new uses of surveillance technologies by their police departments.[32] But all of these share a similar premise: that algorithmic accountability address a *technological process* that requires new forms of regulation in order to be implemented fairly. These are solutions for fixing machines. What if we started somewhere else?

## III. A DIFFERENT FRAMING: EXPERIMENTATION

The ethical review of research involving people today is standardized and grounded in historical experience. Biomedical and behavioral research involving human subjects is generally subject to institutional review boards that focus on the potential ethical consequences of that work. Federally funded research must abide by federal regulations regarding human subjects, including informed consent procedures.[33] "Human subjects" refers to any "living individual about whom an investigator" then obtains "information or biospecimens through intervention or interaction with the individual and uses, studies, or analyzes the information," or does the same for "identifiable private information."[34] Additionally, research is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[35]

Heavily influential to the system for protecting human research subjects today is a report written in 1978 by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.[36] Also known as the Belmont Report, the Commission's work was prompted by notorious abuses of human research subjects, including the 1972 reporting on

[32] *See, e.g.*, ARI CHIVUKULA & TYLER TAKEMOTO, LOCAL SURVEILLANCE OVERSIGHT ORDINANCES 1 (2021), https://www.law.berkeley.edu/wp-content/uploads/2021/02/Local-Surveillance-Ordinances-White-Paper.pdf [https://perma.cc/9ZD3-7G5X] (counting sixteen American jurisdictions that have "passed local surveillance technology oversight ordinances meant to bring more transparency and democratic control to local government use of surveillance technology").

[33] The Federal Policy for the Protection of Human Subjects, first published in 1991, is also referred to as the "Common Rule" and can be found in the Department of Health and Human Services (HHS) regulations at 45 C.F.R. § 46. The Common Rule was updated in 2018. *See, e.g.*, Jerry Menikoff et al., *The Common Rule, Updated*, 376 NEW ENG. J. MED. 613 (2017).

[34] 45 C.F.R. § 46.102(e)(1).

[35] *Id.* § 46.102(*l*).

[36] Eli Y. Adashi, LeRoy B. Walters & Jerry A. Menikoff, *The Belmont Report at 40: Reckoning with Time*, 108 AM. J. PUBLIC HEALTH 1345, 1345 (2018).

the infamous Tuskegee Study.[37] In that experiment, the U.S. Public Health Service offered to treat 600 African American men "for bad blood" in exchange for meals, medical exams, and burial insurance.[38] They were not informed that the actual purpose of the study was to examine the effects of untreated syphilis, and were denied access to a cure. In writing the Belmont Report, the Commission took the view that "risk-laden, albeit promising research" might not be justified "merely on the strength of its potential social benefits."[39]

The hallmarks of the Belmont Report are its three fundamental principles: respect for persons, beneficence, and justice. A respect for persons includes the assumption that "individuals should be treated as autonomous agents" whose "considered opinions and choices" are entitled to respect.[40] Beneficence requires efforts to secure the "well-being" of research subjects, including maximizing possible benefits and minimizing possible to harms to them.[41] The third principle the Report emphasizes is justice: that "an injustice occurs when some benefit is entitled without good reason or when some burden is imposed unduly."[42]

For human subjects research, these three principles translate into practical steps: the use of informed consent by research subjects, a risk/benefit assessment about whether to perform the research, and the careful selection of subjects. As to this final concern, the Belmont Report raises this note of caution:

> Injustice may appear in the selection of subjects . . . . Thus 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.[43]

[37] Also influential before the Belmont Report were the Nuremberg Code and the Declaration of Helsinki, each a framework for ethical considerations in research on human subjects. *See, e.g.*, Kaille Kodama Muscente*, Ethics and the IRB: The History of the Belmont Report*, TEACHERS COLLEGE COLUMBIA UNIVERSITY (Aug. 3, 2020), https://www.tc.columbia.edu/institutional-review-board/irb-blog/the-history-of-the-belmont-report/ [https://perma.cc/WHD5-25N2].

[38] *The Tuskegee Timeline*, CENTERS FOR DISEASE CONTROL AND PREVENTION (Apr. 22, 2021), https://www.cdc.gov/tuskegee/timeline.htm [https://perma.cc/C3C8-AXFL].

[39] *See* Adashi et al., *supra* note 36.

[40] NAT'L COMM'N FOR THE PROT. OF HUM. SUBJECTS OF BIOMEDICAL AND BEHAV. RSCH., THE BELMONT REPORT 4–5 (1979).

[41] *Id.* at 5.

[42] *Id.* at 6.

[43] *Id.* at 9.

These three considerations—respect for persons, beneficence, and justice—are useful rubrics for thinking about the ethics of technology in policing. The technologies on which the police increasingly rely all promise advances in how investigations are conducted. But their costs, whether through mistaken arrests and stops or pervasive surveillance, have yet to find a meaningful ethical framework.

## IV. AUTOMATION, BIOETHICS, POLICING

How can such a very different conversation on law and policy regarding human subject research inform the one in police automation? The algorithmic accountability movement has offered many proposals to address the problems of automation. But these conversations focus first on the technology: how to modify, reform, and monitor both the data and design of automated decision-making. All of this remains important. But to pose the question as the beginning of this Article: what if we think of new forms of automated decision-making in policing as experiments on communities that might impose harms with life altering decisions?[44]

First, we know that surveillance of all kinds is distributed unevenly in society. Receipt of public benefits can often require subjection to drug tests, fingerprinting, verification requirements, and privacy-intrusive questions.[45] Non-white, low-income communities are more often subjected to heavy-handed police presence and surveillance than their wealthier and whiter counterparts.[46] Online, low-income Americans face disadvantages because they usually buy less expensive digital devices with fewer privacy protections and possess fewer digital skills to keep their information private.[47] Low-wage

[44] *Cf.* Kate Crawford & Ryan Calo, *There Is a Blind Spot in AI Research*, NATURE (Oct. 13, 2016), https://www.nature.com/news/there-is-a-blind-spot-in-ai-research-1.20805 [https://perma.cc/H5GT-QJ5U] (noting "there are no agreed methods to assess the sustained effects of such applications on human populations").

[45] Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J. L. & GENDER 113, 114–116 (2011) (discussing Medicaid); Virginia Eubanks, *Want to Predict the Future of Surveillance? Ask Poor Communities*, THE AMERICAN PROSPECT (Jan. 15, 2014), https://prospect.org/power/want-predict-future-surveillance-ask-poor-communities./ [https://perma.cc/FP2E-6JL6] ("Poor and working-class Americans already live in the surveillance future.").

[46] LORI BETH WAY & RYAN PATTEN, HUNTING FOR "DIRTBAGS" 3 (2013) ("[T]hrough discretionary proactive policing (done in their 'free time'), law enforcement officers monitor the lower classes to a greater degree than the middle and upper classes. Such police behavior feeds the cycle of depositing the poor into the criminal justice system and ensuring they remain under criminal justice scrutiny").

[47] *See* Mary Madden, Michele Gilman, Karen Levy & Alice Marwick, *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 62 (2017) (noting that the poor are increasingly online but face privacy and security disadvantages).

work is particularly subject to tracking about movements, productivity, drug tests, and other forms of surveillance.[48]

In addition, non-white, low-income communities are not just subjected to more surveillance, but also more *combinations* of surveillance than other groups.[49] The potential harms from living with pervasive and inescapable surveillance are quite real.[50] People in low-income communities can find it difficult to protect their privacy and to correct mistakes that lead to adverse decisions in housing, credit, and policing. This means some communities live with less autonomy and freedom from surveillance than other groups do.

In the case of policing, we might consider the decision to "test" out a new automated decision-making on a community as a form of experimentation with impacts that might benefit from the ethical concerns in human subjects research. When a law enforcement agency decides to pilot or adopt automated decision-making today, it might do so without informing or receiving consent or input from the community policed; without explicit consideration of whether the experiment maximizes benefits while minimizing harms; or without considering whether a program unduly burdens that community. We would not condone a medical experiment on a community with potential psychological and physical impacts without ethical approvals. But none of the ethical principles fundamental to human subjects research are usually considered for new policing technologies.

The absence of such ethical considerations is striking when we know that police departments do in fact experiment with and sometimes have abandoned automated decision-making programs that have significantly impacted the communities affected. Consider two recent examples.

In 2012, the Chicago Police Department began to use risk models, popularly described as its "Heat Lists,"[51] to identify those who were likely to become victims or perpetrators of gun violence within the next eighteen months.[52] A research team from the Illinois Institute of Technology created the risk models and calculated the "scores" for individuals—everyone who had

[48] *Id.* at 60.

[49] *See id.* at 63 ("It is also important to recognize that for the poor, overt and covert surveillance systems interact with one another.").

[50] *Id.* at 61.

[51] John S. Hollywood, *CPD's "Heat List" and the Dilemma of Predictive Policing*, RAND: THE RAND BLOG (Sept. 21, 2016), https://www.rand.org/blog/2016/09/cpds-heat-list-and-the-dilemma-of-predictive-policing.html [https://perma.cc/RN2C-QVT6] (noting that CPD's Strategic Subjects List was "known colloquially as the 'heat list' ").

[52] CITY OF CHI. OFF. OF INSPECTOR GEN., ADVISORY CONCERNING THE CHI. POLICE DEP'T'S PREDICTIVE RISK MODELS 1 (2020) [hereinafter OIG REPORT].

been arrested in four years before the calculations were made.[53] The higher the risk score, the higher chance that a person would become a "Party to Violence," either as a victim or perpetrator of gun violence.[54] These scores were available to all Chicago Police Department personnel, as well as on its crime mapping software.[55] By 2018, there were nearly 400,000 people with individualized risk scores under the program. The majority of black men in Chicago between the ages of 20 and 29 had a risk score under the program.[56]

It its 2020 report, the City of Chicago's Inspector General found the department's predictive program filled with "concern[s]."[57] The individualized scores and risk tiers used in the program were found to be "unreliable."[58] In addition, the scores, premised on arrests that did not necessarily lead to conviction, may have been the basis of police interventions that "effectively punished individuals for criminal acts for which they had not been convicted."[59] Having a high risk score may have led to some people receiving harsher charging decisions in subsequent arrests, even if they had never been convicted for the prior arrest.[60] The Department formally decommissioned the program in November 2019.[61]

The risk assessment program used in Chicago is an example of reckless automation. Armed with a new data-driven project and $3.8 million dollars in federal funding, the police department experimented with a program that led to numerous "Custom Notification Program" interventions: visits to the homes of persons identified as high risk.[62] These visits were formally described as opportunities to connect high-risk persons to social service programs, but

[53] *Id.* at 2.

[54] *Id.* at 1.

[55] *Id.*

[56] Yana Kunichoff & Patrick Sier, *The Contradictions of Chicago Police's Secretive List*, CHICAGO MAGAZINE (Aug. 21, 2017), https://www.chicagomag.com/city-life/august-2017/chicago-police-strategic-subject-list/ [https://perma.cc/LF9T-44WP].

[57] OIG REPORT, *supra* note 52, at 4.

[58] *Id.*

[59] *Id.* at 7.

[60] *Id.*

[61] *Id.* at 1.

[62] *Id.* at 1–3; *see also* ANDREW G. FERGUSON, THE RISE OF BIG DATA POLICING 38 (2017) (noting these visits involve "a home visit, usually by a senior police officer, a social worker, and a member of the community . . . During the visit, police hand deliver a 'custom notification letter' detailing what the police know about the individual's criminal past, as well as a warning about the future").

in many cases may have been no more than "going door-to-door notifying potential criminals not to commit any violent crimes."[63]

Consider another example: the mistaken arrest of Robert Julian-Borchak Williams.[64] Detroit police had been investigating the theft of $3,800 worth of watches from a local store in 2018. An examiner for the Michigan state police uploaded a still image from the store's surveillance video to the state's facial recognition database. The system would have searched for potential matches in a database of 49 million photos. The facial recognition technology used in this investigation was supplied by a private company that began as a mugshot management software company, which then added facial recognition tools developed by subcontractors.[65] But the private company that contracts with the state does not measure these systems for accuracy or bias.

In Williams's case, the Detroit police would have received a report with potential matches generated by the software. Algorithms incorporated into the software used in the case were also found in a 2019 federal study to have significant inaccuracies in identifying African-American and Asian faces as compared to Caucasian ones.[66] A store employee identified Williams from a photo lineup generated from that report. Confronted with the video still, Williams asked: "You think all black men look alike?"[67] Detroit detectives eventually acknowledged that they arrested the wrong person. But that admission came after Williams had been handcuffed and arrested at home in front of his wife and daughter, had his mug shot, fingerprints, and DNA sample taken, and had been held overnight in jail in 2020.[68] Williams subsequently sued the Detroit police for his wrongful arrest.[69]

The pivotal role of facial recognition in this widely publicized wrongful arrest will be discussed with the terms of algorithmic accountability, but it is also an example of reckless automation that harms the principles of respect for

[63] 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/ [https://perma.cc/YS3R-EL9Z].

[64] The facts here are taken extensively from Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/9KZS-D3CN].

[65] *See id.*

[66] *See id.* (citing NAT'L INST. OF STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/R4DH-VTJJ]).

[67] *See id.*

[68] *See id.*

[69] Drew Harwell, *Wrongfully Arrested Man Sues Detroit Police Over False Facial Recognition Match*, WASH. POST (Apr. 13, 2021), https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/ [https://perma.cc/AF3U-SSBV].

persons, beneficence, and justice. Should the police in Michigan have decided to use an automated system which was demonstrated to make racially disproportionate mistakes, and thus harms, to people? Does such a decision respect the autonomy of persons affected? Can we conclude that such a decision demonstrates attention to "fair procedures and outcomes" affecting the groups and individuals involved?[70] Was there special attention to the fact that any potential harms and mistakes would affect racial minorities disproportionately?[71]

## V. CONCLUSION

The growing calls for algorithmic accountability in the tools of artificial intelligence merit the attention they received. These calls for attention to bias, secrecy, and inaccuracy have special importance in the use of artificial intelligence in policing, where mistakes and biases can impose life-altering consequences. But these approaches share a common premise: that we need fix the problems of these technological tools. Improve the machines, and we improve automated decisionmaking. Until and unless these reforms happen, however, there are people subjected to and harmed by these flawed decisions.

Consider a different perspective: characterizing some adoptions of artificial intelligence in policing as reckless automation that might benefit from the conversations in human subjects research ethics. The long history of ethical lapses in human subjects research has prompted a robust framework that asks fundamental questions about individual consent, community impact, minimizing harms, and special attention to racial minorities, among other groups. The algorithmic accountability conversation brings an important perspective about *technological processes* to policing. This Article urges that a bioethical perspective can offer a perspective on the *human impacts* of policing automation. Even in an age of automation, people remain most important.

[70] *See* BELMONT REPORT, *supra* note 40, at 9.

[71] *See id.* ("One special instance of injustice results from the involvement of vulnerable subjects. Certain groups, such as racial minorities, the economically disadvantaged, the very sick, and the institutionalized may continually be sought as research subjects, owing to their ready availability in settings where research is conducted. Given their dependent status and their frequently compromised capacity for free consent, they should be protected against the danger of being involved in research solely for administrative convenience, or because they are easy to manipulate as a result of their illness or socioeconomic condition.").