ACLU Colorado

2025 Report

Law Enforcement in the Age of AI

Challenges, Implications, and Recommendations

Introduction

The adoption of artificial intelligence (AI) by law enforcement agencies has accelerated dramatically in recent years. Predictive policing programs, facial recognition systems, automated license plate readers, risk assessment algorithms, and administrative tools are now commonplace across Colorado. These applications have been justified by claims about enhanced efficiency, reduced crime, and more strategic resource allocation.

But the use of AI in policing raises constitutional concerns. Law enforcement use of AI undermines equal protection by embedding and perpetuating racial bias; it threatens privacy and liberty interests protected under the Fourth Amendment; and it erodes procedural due process by introducing opaque, black box technologies into criminal justice decision-making. Plus, AI policing programs often require significant public expenditures, despite limited evidence of effectiveness. This creates a cycle of wasteful spending that diverts taxpayer funds from proven community safety strategies. And some critics assert that AI applications use tax dollars to respond to crime, rather than prevent it. Without robust oversight and safeguards, the use of AI in policing may entrench unconstitutional practices and drain scarce public resources.

Equal Protection and Algorithmic Discrimination

Perhaps the most pressing constitutional issue regarding law enforcement use of AI is its potential to reinforce systemic racial bias. Predictive policing tools, facial recognition databases, and risk assessment algorithms are often trained on historical policing data. This data reflects decades of racially discriminatory practices, including disproportionate stops, arrests, and searches in minority communities. When this biased data is fed into algorithmic systems, the outputs have been shown to replicate and intensify patterns of over-policing.[1]

Scholars have described this as a feedback loop: biased policing generates biased data, which informs predictive models that direct police back to the same communities, perpetuating inequity. Recent research has demonstrated that predictive policing systems trained on drug arrest data concentrated police patrols to minority neighborhoods, despite research showing that drug use is relatively consistent across racial groups.[2] By embedding discrimination into ostensibly neutral technology, law enforcement effectively codifies bias into its operations.

This practice is constitutionally questionable under the Fourteenth Amendment's Equal Protection Clause. Although the U.S. Supreme Court has traditionally required proof of discriminatory intent to establish an equal protection violation,[3] AI complicates this analysis. Algorithms may lack "intent" in the human sense, but their discriminatory effects are undeniable. Some experts argue that courts must evolve to recognize disparate impact in the AI context, or risk allowing structural racism to be laundered through technology.[4] Without doctrinal reform, AI threatens to reinforce inequality while escaping constitutional scrutiny.

Fourth Amendment Challenges in the Age of AI

The Fourth Amendment protects against unreasonable searches and seizures, but its application to AI-enhanced surveillance remains largely unsettled. Facial recognition technology, automated license plate readers, and predictive analytics enable law enforcement to monitor individuals at a scale previously unimaginable. Scholars have likened these tools as creators of a "perpetual line-up," where citizens can be identified and tracked continuously without their knowledge or consent.[5]

Traditional doctrine is ill-equipped to handle such developments. Case history indicates potential pathways for pursuing strengthened data surveillance protections. In *Katz v. United States*, the U.S. Supreme Court held that the Fourth Amendment protects people, not places, and introduced the "reasonable expectation of privacy" test.[6] Courts have struggled to apply this test to emerging technologies, but some cases have set meaningful precedents. In *United States v. Jones*, the Court recognized that attaching a GPS tracker to a vehicle for prolonged surveillance constituted a search, suggesting that duration and intrusiveness matter.[7] In *Carpenter v. United States*, the Court held that accessing cell site location information required a warrant, emphasizing that technological advances should not erode constitutional protections.[8]

AI surveillance raises parallel concerns. Continuous facial recognition in public spaces, for example, allows law enforcement to reconstruct an individual's movements and associations over time. This mirrors the concerns raised in *Carpenter* about pervasive location tracking. Yet, unlike GPS or cell site data, AI surveillance may not require physical intrusion or third-party records, making it harder to fit within traditional doctrine. The risk is that courts will treat AI monitoring as permissible because it occurs in public, despite its intrusive and comprehensive nature. Without doctrinal innovation, the Fourth Amendment may fail to protect against the uniquely invasive capabilities of AI.

Due Process, Transparency, and the Black Box Problem

AI technologies also threaten procedural due process. Many systems operate as black boxes, whose internal logic is inaccessible to defendants, lawyers, and even judges. Proprietary algorithms, such as those used in risk assessment tools and predictive policing software, are often shielded by trade secrecy claims. As a result, defendants cannot scrutinize or challenge the accuracy of the evidence used against them.[9]

This lack of transparency undermines fundamental fairness. Due process requires notice of the evidence used in proceedings and a meaningful opportunity to contest it.[10] When courts admit AI-generated results without disclosing the methodology, defendants are deprived of this opportunity. Danielle Keats Citron, legal scholar with the University of Virginia School of Law, described this phenomenon, in a Washington University Law Review, as the erosion of "technological due process," in which bureaucratic decisions are automated and insulated from challenge.[11]

Real-world examples illustrate the dangers. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) risk assessment tool, a software that algorithmically assesses potential recidivism risk and is used in sentencing and bail determinations, has been criticized for racial bias and lack of transparency.[12] In *State v. Loomis*, the Wisconsin Supreme Court upheld the use of COMPAS, but acknowledged serious constitutional concerns, including potential violations of due process.[13] This case demonstrates how AI tools are infiltrating the justice system even as their reliability and fairness remain unproven.

Law-enforcement use of AI in Colorado

Colorado law enforcement agencies are implementing a range of AI-powered tools that affect investigations, surveillance, and routine policing work. Tools already in use, or under active consideration, include automatic license-plate readers that digitize and index vehicle movement; drones used as first responders and to conduct patrols; and productivity automation tools that can draft reports, extract information from body-cameras, or dispatch recordings.

Facial recognition technology is also increasingly being used. While recent local reporting shows only a small number of Colorado agencies are fully authorized for Facial Recognition Services (FRS) use, several others.[14]

Colorado's legal and policy framework continues to evolve slowly when it comes to law enforcement's use of AI. The state passed targeted restrictions and governance for facial recognition in 2022 (Senate Bill 22-113), which prohibits certain live/ongoing surveillance uses and requires training, record-keeping, and limits on using FRS results as the sole basis for probable cause.[15]

For now, FRS operational practices vary by jurisdiction. Colorado law permits facial recognition in investigations under constrained conditions (warrants, defined investigative needs, or court orders for narrow purposes), and agencies must maintain FRS policies and training. Still, local debates and council votes show political, and community scrutiny is shaping deployment decisions in 2024–2025.[16]

Several jurisdictions are also adopting AI productivity tools that commanders say reduce time spent on paperwork, which agencies present as efficiency gains even while civil-liberties groups warn of accuracy, bias, and oversight risks.

Through Colorado Open Records Act requests to local law enforcement agencies in different geographical locations across the state, the ACLU of Colorado was able to identify some AI use trends. Several AI systems used for reporting and recording redaction, transcription, and translation, like Axon's Auto Transcribe[17] and Draft One[18] and Truleo[19] are used across urban and rural areas alike. As police reports play a crucial role in our justice system, AI bias and unreliability can cause issues that have lasting impacts. We risk losing not only accuracy and transparency in the discovery process, but also accountability and human judgment that are essential to fair policing. When reports are generated, or heavily influenced, by artificial intelligence, the nuanced reasoning behind an officer's decisions — especially in moments involving discretionary use of force — can disappear into algorithmic opacity. The human act of writing a report is itself a form of reflection and discipline: it requires officers to recall events, justify their actions, and articulate their decision-making in a way that can later be scrutinized. This process helps ensure both integrity and accountability.

In contrast, when AI automates this documentation, officers lose the opportunity to explain their exercise of discretion in their own words, whether to protect themselves from false accusations or to be held accountable for misconduct. Automated reports may produce polished, standardized narratives, but they obscure the messy realities of human judgment and the situational factors that shape each encounter. Without human-authored documentation, it becomes far more difficult for investigators, courts, and communities to trace the reasoning behind police actions or to identify patterns of bias and abuse.

Of the 246 law enforcement agencies across the state, more than 80 — over one-third — have contracts with Flock Safety, an automated license plate reader (ALPR) platform. In addition to collecting license plate numbers from passing cars, it can also flag when a car is on what Flock and law enforcement call a "hotlist," and can search for vehicles using either a license plate number or unique descriptors such as make, model, color, dents, and bumper stickers. Flock has also created a nationwide network where local law enforcement agencies can search to find cars in other jurisdictions — a practice that could violate Colorado law under SB25-276 if those searches are used for immigration enforcement.[20]

Over one third of law enforcement agencies in Colorado have contracts with Flock Safety.

Source: ACLU of Colorado

Drones are also being used across the state for many purposes. Some agencies, like the Pagosa Springs Police Department, have been awarded Persons Who Wander grant dollars from the Colorado Bureau of Investigation to purchase drones to assist in search and rescue efforts for individuals with dementia and other conditions that affect their awareness.[21] There is no requirement, however, that drones purchased with these funds are used solely for the grant program's stated purpose — and many agencies use drones for general patrolling and surveillance purposes as well. Due to their ability to record audio- and video and produce heat maps in areas that would not otherwise be viewable to officers, drones have been used to surveille private areas protected by the Fourth Amendment. Left unchecked and unregulated, drone use risks violating constitutionally protected privacy rights.

Fiscal Costs and the Burden on Taxpayers

Beyond constitutional issues, AI policing imposes significant costs on taxpayers. Contracts for data analytics platforms and FRSs often involve millions of dollars in public expenditures. Yet, studies repeatedly show that these technologies fail to deliver promised results.

The city of Chicago, for example, spent more than $2 million on its Heat List, a PredPol (predictive policing) program intended to identify individuals most likely to be involved in gun violence. But independent evaluations concluded that the program was ineffective and raised concerns about stigmatizing individuals without due process.[22] Similarly, New Orleans partnered with Palantir to implement predictive policing, only to end the contract amid criticism of secrecy, questionable efficacy, and cost.[23] The Los Angeles Police Department also abandoned its PredPol program after audits revealed little evidence of effectiveness and amid growing concerns about bias.[24]

These expenditures are not one-time costs. AI systems require continuous licensing, software updates, and vendor support. This creates long-term financial obligations that lock municipalities into expensive contracts. The opportunity costs are equally troubling. Funds spent on unproven AI tools could instead support community-based violence prevention, housing, education, or mental health services — investments with a demonstrably greater impact on public safety.[25] In this way, AI-powered policing not only wastes taxpayer dollars, but also diverts resources from strategies that address the root causes of crime.

AI systems create multiple budgetary impacts for local and state governments. Those costs fall into direct procurement/operational spending, continuing maintenance and staffing/training, legal and settlement exposure, and indirect administrative/compliance burdens. Below are the principal cost drivers:

Upfront procurement and annual operating costs.

ALPR programs commonly run into the low-to-mid six figures for citywide contracts: a recent Denver proposal to extend a Flock ALPR contract was roughly $666,000 for two years and drew public pushback; individual commercial ALPR services are often priced in the thousands per camera, per year.[26]

Through Colorado Open Records Act requests, the ACLU of Colorado was able to gain information related to these upfront costs for several agencies across the state:

- *Avon Police Department:* Over $53,000 anually for Axon, CaseGuard, Dronesense, Flock, and Truleo contracts
- *Colorado Springs Police Department:* Over $3.6 million annually for Flock, Axon, and red light and speeding enforcement contracts
- *Prowers County Sherriff's Office:* Over $23,000 since 2021 for drones and accessories
- *Routt County Sherriff's Office:* Has a $35,000 annual Flock contract, and a $53,497.50 contract with Axon for 21 months for AI assisted transcription and report drafting

Ongoing staffing, training, and audit costs.

Colorado law now mandates training, documented policies, and recordkeeping for FRS and biometric processing — meaning agencies must budget for personnel time, external audits, and data-protection assessments. Even where tools promise efficiency (e.g., AI that drafts police reports), agencies must invest in onboarding, quality control, and oversight of staff to validate AI outputs and comply with transparency rules.[27]

Litigation and settlement exposure.

Misuses or errors in biometric/AI systems have led to costly settlements and payouts. Examples include wrongful-arrest settlements tied to facial-recognition errors (with reported settlements in the low-to-mid six figures in some cases), and the high-profile Clearview litigation that produced a novel settlement structure potentially worth up to $51.75 million.[28]

Data storage, retention, and compliance costs.

Biometric datasets and ALPR feeds require secure, often long-term, storage that can be costly, especially for smaller agencies, without which there is an increased risk of data breaches.

Opportunity and community costs.

Public backlash against surveillance purchases can force cancellations (as Denver's City Council did in May 2025), or lead to task-force creation or extended public engagement processes — each of which has administrative and political costs.

Along with contracts and purchase orders, the ACLU of Colorado also requested any documentation of audits performed on any AI systems they may be using — a low bar for transparency and accountability when using these systems. We received no audits, and no confirmation that any audits on these systems are occurring.

Additionally, wrongful arrests or biased outcomes impose societal costs (such as lost work, legal defense funds, settlements) and reduce public trust — costs that are often borne indirectly by taxpayers.[29]

Policy and Legislative Implications

Given the constitutional and fiscal challenges, policymakers must reconsider the role of AI in law enforcement. Several jurisdictions have already acted. San Francisco, Boston, and Portland have banned government use of facial recognition, citing privacy and civil rights concerns.[30] At the federal level, legislative proposals have called for algorithmic audits, transparency requirements, and limits on the use of AI surveillance.[31] Internationally, the European Union has advanced the AI Act, which imposes stricter regulations on high-risk AI systems, including those used in law enforcement.[32]

These reforms point toward a broader principle: AI policing must be subject to democratic oversight and constitutional limits. Courts should require warrants for AI surveillance akin to those mandated in *Carpenter*. Lawmakers should mandate transparency, including public disclosure of contracts, algorithms, and performance metrics. Independent audits should evaluate both accuracy and discriminatory impacts. And fiscal accountability must be prioritized to ensure that taxpayer dollars are directed toward effective, equitable public safety strategies rather than unproven technologies.

Policy Recommendations

Transparency and Accountability

- Require a transparent process prior to use or continued use of AI technologies in law enforcement, inclusive of a community input process.
- Allow full public access to AI contracts, vendor agreements, and independent audits.
- Mandate algorithmic audits to assess bias, accuracy, and constitutional compliance.
- Ensure reasonable statutory retention schedules for storing data.

Constitutional Safeguards

- Establish warrant requirements for AI-enabled surveillance, including facial recognition.
- Prohibit the use of predictive policing tools that rely on biased historical data.
- Guarantee defendants access to algorithmic methodologies and datasets in criminal proceedings.

Fiscal Responsibility

- Require cost-benefit analyses before adoption of AI technologies.
- Sunset provisions for AI contracts, requiring periodic legislative review.

- Redirect funding toward community-based violence prevention, public health, housing, and behavioral and mental health services.

Legislative and Regulatory Action

- Enact state-level moratoria on facial recognition until constitutional safeguards are in place.
- Develop statewide standards for law enforcement use of AI.
- Support local governments in creating oversight boards with community representation.

Conclusion

The integration of AI into law enforcement raises profound constitutional and fiscal concerns. Predictive policing and surveillance technologies threaten equal protection, erode Fourth Amendment privacy rights, and undermine due process through opaque decision-making. At the same time, municipalities spend taxpayer dollars on systems that consistently fail to deliver promised outcomes. The result is a policing landscape that is more invasive, less accountable, and fiscally irresponsible.

Unless meaningful safeguards are imposed, AI policing risks entrenching discriminatory practices and diverting scarce resources from more effective alternatives. Constitutional fidelity and fiscal responsibility require a reevaluation of AI's role in law enforcement. To protect civil liberties and promote efficient governance, policymakers and law enforcement agencies must resist the allure of technological quick fixes and instead pursue strategies that align with democratic values and constitutional principles.

Endnotes

1 Rashida Richardson, Jason Schultz & Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (2019).

2 Kristian Lum & William Isaac, To Predict and Serve?, 13 Significance 14 (2016)

3 Washington v. Davis, 426 U.S. 229 (1976).

4 Bains, C., (September 13, 2024), The Legal Doctrine that will be Key to Preventing AI Discrimination, Brookings, https://www.brookings.edu/articles/the-legal-doctrine-that-will-be-key-to-preventing-ai-discrimination/#:~:text=Disparate%20impact%20liability%20helps%20root,helps%20smoke%20out%20intentional%20discrimination.

5 Clare Garvie, Alvaro Bedoya & Jonathan Frankle, The Perpetual Line-Up: Unregulated Police Face Recognition in America (2016).

6 *Katz v. United States*, 389 U.S. 347 (1967).

7 *United States v. Jones*, 565 U.S. 400 (2012).

8 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

9 Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (2017).

10 U.S. Const. amend. V; amend. XIV.

11 Danielle K. Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249 (2008).

12 Julia Angwin et al., Machine Bias, ProPublica (2016).

13 State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

14 Goodland, M. (2023, October 16). Colorado police explore AI tools, from report-writing to facial recognition. Colorado Newsline. https://coloradonewsline.com

15 Colorado General Assembly. (2022). SB22-113: Restrictions on governmental use of facial recognition services. https://leg.colorado.gov/bills/sb22-113

16 Denver City Council. (2025, May 13). Council proceedings: Vote on Flock ALPR contract extension. City and County of Denver, Legislative Council Records.

17 Auto-Transcribe - Axon.com

18 Draft One - Axon

19 TRULEO | Patrol: Smarter Shifts with AI Support

20 2025a_276_signed.pdf

21 Pagosa Springs Police Department awarded Persons Who Wander grant - The Pagosa Springs Sun

22 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 (2016).

23 Ali Winston, Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology, The Verge (Feb. 27, 2018).

24 LAPD Inspector General, Audit of PredPol Program (2020).

25 Patrick Sharkey, Uneasy Peace: The Great Crime Decline, the Renewal of City Life, and the Next War on Violence (2018).

26 Murray, J. (2025, May 14). Denver City Council votes down $666K ALPR contract with Flock Safety. Denver Gazette. https://denvergazette.com

27 Colorado Attorney General's Office. (2024). Biometric data and privacy rulemaking under the Colorado Privacy Act. https://coag.gov

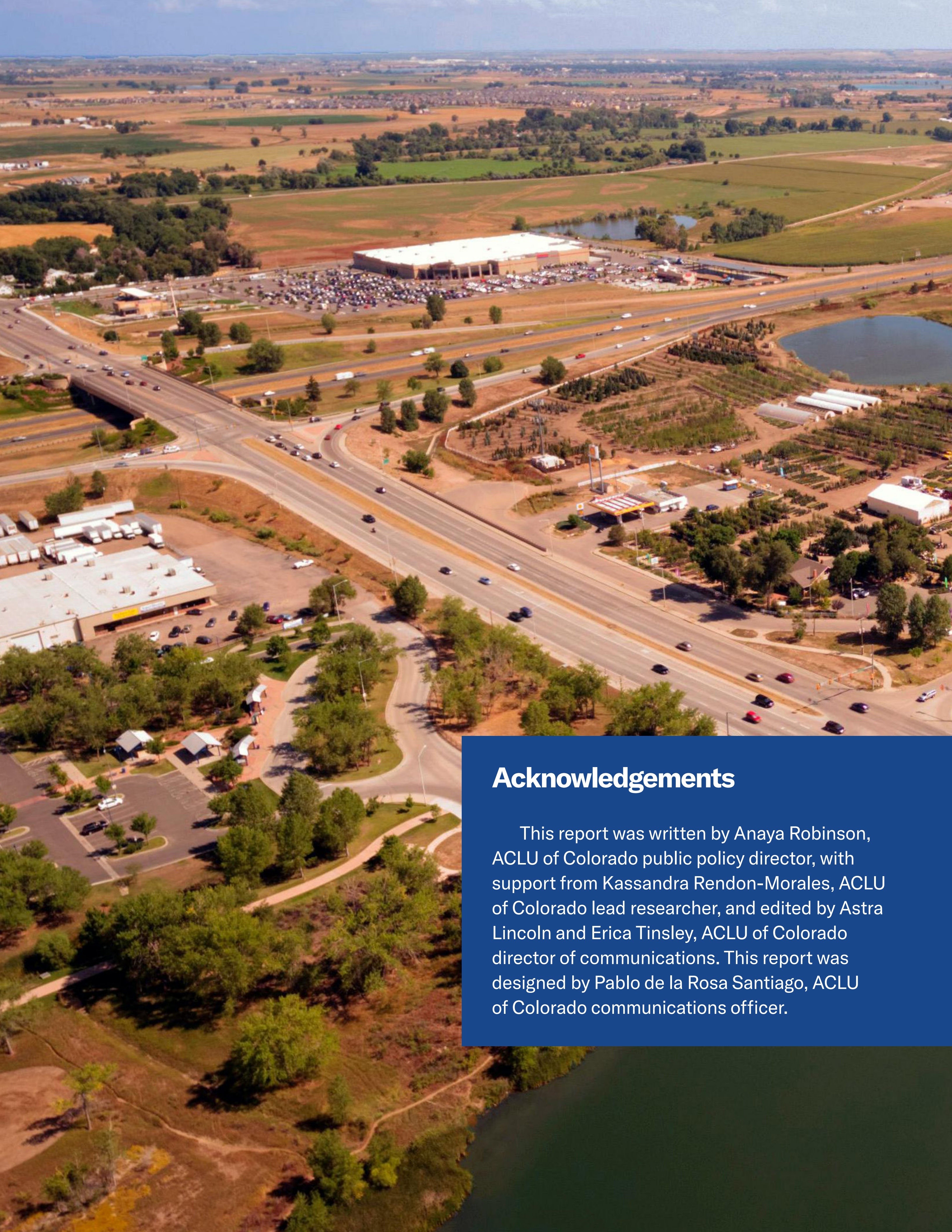
28 Singer, N. (2024, May 3). Clearview AI settles class action lawsuit for up to $51.75 million. New York Times. https://nytimes.com

29 Prentzel, K. (2025, May 15). Denver council halts ALPR expansion amid privacy and bias concerns. Denver Post.

30 City of San Francisco, Ordinance No. 103-19 (2019); City of Boston, Ordinance Banning Government Use of Face Surveillance (2020); City of Portland, Ordinance No. 190114 (2020).

31 Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. (2022).

32 European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act), COM/2021/206 final.



Acknowledgements

This report was written by Anaya Robinson, ACLU of Colorado public policy director, with support from Kassandra Rendon-Morales, ACLU of Colorado lead researcher, and edited by Astra Lincoln and Erica Tinsley, ACLU of Colorado director of communications. This report was designed by Pablo de la Rosa Santiago, ACLU of Colorado communications officer.

ACLU
Colorado

Denver, CO
aclu-co.org
@acluofcolorado