



Navigating a Brand New Landscape: Technology in the Criminal Justice System

Policy Leads: Naomi McKenna, Aditi Karthikeyan

Policy Analysts: Afomiya Dejene^{#2}, Alan Le^{#3}, Mehek Saini^{#4}, Sophie Chan^{#5}, Rohan Manchada^{#6}

Criminal Justice Policy Team, Institute for Youth in Policy

naomi@yipinstitute.org, aditik@yipinstitute.org,

Abstract:

This brief examines the effects of automated surveillance systems on the criminal justice landscapes. It focuses on concerns surrounding recent technological developments in the landscape of surveillance and proposes policy options protecting against potential risks.

Keywords — surveillance, automation, facial recognition, technology, privacy, artificial intelligence

I. EXECUTIVE SUMMARY

In 2024, the Cybersecurity and Infrastructure Security Agency released an advisory warning on Motorola Solutions' Automated License Plate Readers (ALPRs), finding seven vulnerabilities from various forms of improper storage or encryption. While automated surveillance has long been contentious within criminal justice, emerging technological advancements such as Artificial Intelligence (AI) systems introduce novel dimensions of risk and privacy that urge a revisitation of these systems' historical roots, societal implications, and policy solutions.

II. OVERVIEW

Although the post-9/11 domestic environment is credited as the most recent mass influx of such technologies, automated surveillance systems date back as far as the late 1970s. However, research shows that the majority of data collection through these

surveillance systems have historically occurred without the users' legislative consent. To restore trust in automated surveillance systems, states must begin to adopt technology-specific restrictions that increase transparency in collection and analysis.

III. HISTORY

With the mass adoption of inventions such as Artificial Intelligence (AI) and Automated License Plate Readers (ALPRs), law and technological advancements are increasingly placed at a crossroads. To understand the nuance and policy implications on citizens and everyday people, it is necessary to understand the history of these developments.

A foundational turning point in privacy jurisprudence arrived with the 1967 Supreme Court ruling in [Katz v. United States](#), which established that the Fourth Amendment protects an individual's "reasonable expectation of privacy" from unlawful surveillance. This rejected the Court's previous ruling that a *nonphysical* trespassing of defendants' property did not constitute a Fourth Amendment search. Shortly thereafter, the late 1970s and 80s marked the birth of automated tracking with the rise of the [ALPRs](#), which initially operated as rudimentary optical recognition tools before evolving into mobile patrol car units and fixed optical networks throughout the 1990s.

The landscape of domestic policing shifted dramatically in the post-9/11 era. An influx of federal grants from the Department of Homeland Security poured billions of dollars into municipal police departments, funding the creation of urban Real-Time Crime Centers and the procurement of advanced biometric technologies. During this period, rudimentary facial recognition algorithms were first deployed on a public mass scale, most notably at [Super Bowl XXXV in 2001](#), where attendees' faces were scanned against law enforcement mugshot databases without prior notice. By the 2010s, deep learning models, cloud computing, and massive driver's license image databases transformed facial recognition technology into a nationwide law enforcement network. A landmark [2016 report on facial recognition](#) by the Georgetown Law Center on Privacy & Technology revealed that over half of American adults were included in police facial recognition search networks often through driver's license photos gathered without explicit legislative consent.

As automated surveillance has expanded from passive recording to proactive tracking, legal scholars have noted that these tools were frequently processed through [opaque administrative processes](#) that bypassed public debate and municipal oversight. In response to continuous location tracking, the judiciary began re-evaluating Fourth Amendment protections in the digital age. In 2012, the Supreme Court held in [United States v. Jones](#) that prolonged automated tracking via GPS devices on vehicles constituted a constitutional search. Six years later, the court built upon this precedent in [Carpenter v. United States](#), ruling that law enforcement must obtain a warrant to access historical digital location data. A [2021 report from the Government Accountability Office](#) documented that dozens of federal law enforcement agencies routinely utilized commercial and non-federal facial recognition databases without standardized privacy safeguards. Today, the

convergence of AI-driven video analytics, predictive algorithms, and automated license plate networks presents unprecedented challenges for balancing public safety with civil liberties.

IV. POLICY PROBLEM

A significant area of inaccuracy regarding automated systems is their frequent reliance on faulty historical data. When AI systems identify and apply patterns, [they operate only within the data that they have been given](#), preventing no safeguard to any biases that may be present in the input. For example, if these systems are fed data reflecting stereotypes in certain populations, the results of the same systems may inaccurately present a result based on those patterns. When applied to technologies such as facial recognition, this may lead to generalization and flawed outcomes.

Furthermore, unlike traditional identification methods, many automated systems do not enforce a necessary verification process within their analyses. Many [algorithmic tools](#) such as those involved with these automated systems can come to a conclusion quickly based on a set of instructions, skipping a critical explanatory process. Policy directly addressing this concern also remains limited: while regulations have attempted to mandate audits of [AI-fed data in situations such as employment](#), they are not yet enforced on critical industries such as automated systems.

Lastly, privacy concerns remain incredibly prevalent in the field of automated systems. Not only do many automated systems fail to explicitly [receive consent from the individuals that they are extracting data from](#), they also have the potential of obtaining more information than what is necessary for their operations. Policy often fails at mandating a disclosure and agreement process with these technologies, especially when they are present in public environments. In order to address these concerns, users should be presented with an opportunity to opt

out of various processes collecting private information and to become cognizant of how their data will be used.

V. POLICY OPTIONS

Policy reform must therefore target the specific risks of automated surveillance technologies that pose due process and civil liberties, ultimately strengthening transparency and democratic oversight.

First, because facial recognition and video analytics are prone to error and easily used as dragnet tools, states should adopt technology specific restrictions including but not limited to:

- i) Requiring independent agency and bias testing before any agency deploys facial technology
- ii) Banning the use of facial recognition match as the sole basis for any arrest or warrant
- iii) Requiring human oversight to match up with any algorithm error with other evidence before acting up on it

While some jurisdictions have already taken these precautions, enforcement gaps persist. [For example, the Detroit Board of Police Commissioners require civilian oversight of facial recognition use, yet the department is tied to at least a dozen wrongful arrests.](#) In several of these cases, law enforcement and police officers ignored obvious physical evidence between the accused and the actual perpetrator including mismatching tattoos, height differences, or advanced pregnancy. This particularly points to the importance of human oversight in bridging potential limitations in algorithm matches.

In addition, states should require transparency and community oversight before agencies acquire or expand surveillance technology. Rules targeting specific technologies will be insufficient if the public and elected officials are not aware of what tools are

already being deployed. Legislatures should require law enforcement agencies to obtain city council approval and publish a surveillance impact report before acquiring new surveillance technology, along with an annual public report on how each tool was used. [The Community Control Over Police Surveillance \(CCOPS\) model, now adopted in 26 jurisdictions, provides a reliable precedent. Rather than discovering their existence after the fact, the CCOPS requires a rigorous, transparent public review process that allows residents to question and reject surveillance proposals before they're implemented.](#)

Finally, states should require stronger accountability mechanisms when surveillance technology contributes to a person's arrest. As a result, these reforms would ensure that this technology is enclosed, disclosed, and independently verified.

VI. CONCLUSIONS

The proliferation of mass surveillance in the wake of the 9/11 attacks, combined with the rise of automated surveillance with AI, is not without its faults. The data used to train these systems relies only on the data and identifies patterns in the data given to the system. Problems arise when the data is based on stereotypes, resulting in generalization when it comes to identifying people with face recognition. Furthermore, privacy concerns are still prevalent as many technologies do not seek user consent. Policy reforms therefore aim to strictly regulate systems, incorporate human evaluation within its processing frameworks, and to offer users an opportunity to opt out of any measures they are not comfortable with.

VII. ACKNOWLEDGEMENT

The Institute for Youth in Policy wishes to acknowledge Donna Kim for editing this policy brief.

VIII. REFERENCES

- [1] American Civil Liberties Union. (2023, August 6). *After third wrongful arrest, ACLU slams Detroit Police Department for continuing to use faulty facial recognition technology* [Press release]. <https://www.aclu-wi.org/campaigns-initiatives/ccops/>
- [2] American Civil Liberties Union. (n.d.). *Community control over police surveillance*. Retrieved July 28, 2026, from <https://www.aclu.org/community-control-over-police-surveillance>.
- [3] Australia Human Rights Commission. 2020. "Historical Bias in AI Systems ." In *Humanrights.Gov.Au*. <https://humanrights.gov.au/about-us/media-centre/media-releases/technology-and-human-rights/historical-bias-ai-systems>.
- [4] Bloch-Wehba, Hannah. "Visible Policing: Technology, Transparency, and Democratic Control." *California Law Review* 109, no. 3 (2021): 917–78. <https://www.californialawreview.org/print/visible-policing-technology-transparency-and-democratic-control>.
- [5] *Carpenter v. United States*, 138 S. Ct. 2206 (2018). <https://epic.org/documents/carpenter-v-united-states-2/>.
- [6] Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. *The Perpetual Line-Up: Unregulated Police Facial Recognition in America*. Washington, DC: Georgetown Law Center on Privacy & Technology, 2016. <https://www.perpetuallineup.org/>.
- [7] Greason, Carrine. 2024. "Ethics in Autonomous Industrial AI: Tackling Bias and Data Privacy." In *Automate*. Association for Advancing Automation. <https://www.automate.org/ai/industry-insights/ethics-in-a-utomated-industrial-ai>.
- [8] *Katz v. United States*, 389 U.S. 347 (1967). <https://constitutioncenter.org/the-constitution/supreme-court-case-library/katz-v-united-states>.
- [9] New America. n.d. "Lack of Transparency and Perceived Objectivity Perpetuate Biases in Algorithmic Tools." In *New America*. Accessed July 26, 2026. <https://www.newamerica.org/insights/automated-intrusion-systemic-discrimination/lack-of-transparency-and-perceived-objectivity-perpetuate-biases-in-algorithmic-tools/>.
- [10] New York City Department of Consumer and Worker Protection. n.d. "Automated Employment Decision Tools (AEDT) ." In *Www.Nyc.Gov*. Accessed July 26, 2026. <https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page>.
- [11] Sikkema, Kelly. "White Rectangular Frame on Brown Wooden Table." Photograph. Published February 3, 2021. Unsplash. <https://unsplash.com/photos/white-rectangular-frame-on-brown-wooden-table-xODSxohNj-w>.
- [12] *United States v. Jones*, 565 U.S. 400 (2012). <https://www.oyez.org/cases/2011/10-1259>.
- [13] U.S. Congressional Research Service. *Law Enforcement and Technology — Use of Automated License Plate Readers*. CRS Report R48160. Washington, DC: Congressional Research Service, 2024. <https://www.everycrsreport.com/reports/R48160.html>.
- [14] U.S. Government Accountability Office. *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*. GAO Report GAO-21-518. Washington, DC: U.S. Government Accountability Office, 2021. <https://www.gao.gov/assets/gao-21-518.pdf>.