

How Technology Has Contributed To The Problems In Criminal Justice

Posted on October 14, 2019

View this essay online:

<https://academic-master.com/how-technology-has-contributed-to-the-problems-in-criminal-justice/>

Introduction

Criminal justice agencies increasingly rely on technology to collect evidence, identify suspects, allocate resources, supervise defendants, and communicate with courts and the public. These tools can improve safety and accuracy, but they can also create new problems when agencies adopt them without clear goals, independent validation, privacy rules, or meaningful oversight. The central issue is therefore not whether technology is good or bad in itself, but how a specific tool changes decision-making inside institutions that already contain legal constraints, unequal enforcement patterns, organizational incentives, and imperfect data. A camera may preserve an encounter without deciding what the footage means. A predictive model may identify a location as “high risk” even when the historical records reflect where police were deployed rather than where all crime occurred. A DNA profile may be scientifically powerful yet still require careful interpretation. Evaluation of criminal-justice technology therefore examines both potential benefits and the institutional conditions under which error, bias, surveillance, or unintended consequences can emerge (Lanier & Cooper, 2016).

From Procurement to Evidence-Based Adoption

An evidence-based adoption model begins with measurable objectives and a definition of the public problem being addressed. A department considering a new application may be attempting to reduce [violent crime](#), improve evidence collection, strengthen complaint review, locate missing people, reduce detention, or increase procedural fairness. The chosen outcome then determines what an evaluation measures. Counting devices purchased, videos uploaded, alerts generated, or searches performed measures activity rather than outcomes. NIJ research emphasizes that criminal-justice technologies produce different results depending on implementation, training, agency culture, local crime patterns, and policy rules (National Institute of Justice [NIJ], 2022). Evaluation frameworks commonly include baseline data, pilot programs, legal review, technical validation, cost analysis, and predefined outcome measures. Independent evaluation is especially relevant when the vendor selling the product also supplies performance claims. These methods allow agencies and communities to compare a technology with existing practice or non-technological alternatives without assuming that procurement itself demonstrates effectiveness.

Cameras, Facial Recognition, and Identification Error

Body-worn cameras illustrate both the promise and the limitations of criminal-justice technology. They can preserve audiovisual evidence, help resolve complaints, support training, and influence behavior in some settings. NIJ's review describes the overall evidence as mixed: some studies report benefits, while others find no effect or possible negative effects, and a major review found no consistent statistically significant impact across several officer-behavior outcomes (NIJ, 2022). Results vary with activation rules, supervisory practices, officer discretion, and consequences attached to recorded conduct. A camera also does not reproduce an entire event. Important actions may occur before activation or outside the field of view, and viewers may interpret the same footage differently. Privacy questions arise when cameras record inside homes, hospitals, schools, or interactions with victims and children. Governance policies therefore vary on activation, notice, retention, redaction, evidentiary access, public release, and disciplinary review. Comparative evaluation can examine cameras alongside de-escalation training, supervision, procedural-justice practices, or community-based interventions.

Facial-recognition systems create a different problem because rapid automated output can be mistaken for a definitive identification. NIST evaluations show that performance varies by algorithm, image quality, threshold, application, and demographic characteristics. NIST's current demographic-evaluation pages report that false negatives are strongly affected by image quality and that false-positive rates can vary across demographic groups even with high-quality images (National Institute of Standards and Technology [NIST], 2019; NIST, 2026). In operational use, a ranked candidate list can function as an investigative lead rather than as proof that a person committed an offense. Policy frameworks differ on requirements for trained human review, documentation of search conditions, independent corroboration, disclosure, and database restrictions. Database choice also changes the privacy and legal questions involved because mugshots, driver-license photographs, passport images, and privately collected images originate under different conditions. The accuracy of an algorithm therefore represents only one part of the analysis; evidentiary reliability also depends on capture quality, search procedures, human interpretation, and how the result is used in later investigation.

Predictive Systems, DNA, and Digital Evidence

Predictive policing and risk-scoring systems can reproduce historical inequalities when administrative records are treated as neutral representations of crime. Recorded incidents reflect where police patrol, which behavior is visible, who reports offenses, how officers classify encounters, and which cases proceed through the system. If a neighborhood receives heavy enforcement, it may generate more recorded low-level crime, which can then become data supporting continued enforcement. This feedback mechanism means predictive accuracy cannot by itself demonstrate that a particular intervention reduces harm. A model may identify where violence is statistically more likely without

determining whether patrol, environmental design, youth services, focused investigation, or conflict mediation would produce the desired result. Risk tools used for bail, sentencing, or supervision raise related questions when variables reflect unequal employment, housing, policing, or access to treatment. Policy analysis therefore examines the source of training data, error distribution, transparency, opportunities to contest information, and the degree to which a human decision-maker can understand or override a model's output (Lanier & Cooper, 2016).

DNA analysis and digital forensics demonstrate that highly useful technologies still depend on procedural reliability. DNA can identify suspects, exclude innocent people, connect cases, identify remains, and support post-conviction review, but laboratories must manage contamination, mixtures, transfer, degradation, statistical interpretation, and chain of custody. The National Research Council's 2009 consensus report documented weaknesses in the scientific foundations and legal treatment of several forensic disciplines and called for stronger validation and research (National Research Council, 2009). Digital investigations create additional challenges because phones, cloud accounts, vehicles, cameras, social media, and location services can contain enormous amounts of private information. Operational controls can include validated tools, trained examiners, secure storage, search limits, audit trails, and methods for separating relevant evidence from unrelated personal data. Software-generated reports also require interpretation: a location point contains uncertainty, an account may be shared, and a message may be sarcastic or removed from context. Technical extraction is therefore only one stage in determining evidentiary meaning.

Privacy, Governance, and Institutional Pressure

Privacy, procurement, and politics influence whether technology strengthens or weakens legitimacy. Agencies may face pressure to purchase visible solutions after a serious crime or controversial incident, while vendors can shape expectations through demonstrations, grants, proprietary claims, and lobbying. Once a department commits to infrastructure, training, contracts, and data integration, abandoning an ineffective product can become more difficult. Transparency frameworks can disclose validation studies, error rates, data-sharing terms, retention rules, cybersecurity responsibilities, and conditions for independent audit. Data-minimization frameworks take a different approach by limiting collection and retention to information tied to a defined purpose. Access controls, logging, and periodic review can reduce unauthorized or secondary use. Community consultation is another governance mechanism, particularly when surveillance is concentrated in specific neighborhoods or populations. These mechanisms address different risks and can be compared through legal compliance, measured outcomes, costs, error patterns, privacy effects, and public perceptions rather than being treated as evidence that any one technology is inherently legitimate or illegitimate (Lanier & Cooper, 2016).

Conclusion

Technology can alter criminal justice substantially without producing the same effects in every institution or community. A common governance sequence includes defining the problem, comparing technological and non-technological alternatives, validating performance under realistic conditions, establishing legal and privacy rules, piloting the system, measuring outcomes, examining differential effects, and deciding whether continued use matches the evidence. This framework can be applied to body cameras, DNA analysis, facial recognition, predictive systems, electronic monitoring, and digital forensics without assuming that all tools deserve the same policy response. Each can generate benefits, but each can also amplify error, surveillance, bias, cost, or institutional overreach under particular conditions. Evaluation can focus on measurable outcomes such as safety, reliability, evidentiary quality, accountability, privacy effects, cost, and public confidence. A broader discussion of emerging tools appears in [criminal justice technology](#). The central analytical question is whether a particular application produces the intended result with acceptable legal, scientific, financial, and social tradeoffs (NIJ, 2022).

References

Lanier, M. M., & Cooper, A. (2016). From papyrus to cyber: How technology has directed law enforcement policy and practice. *Criminal Justice Studies*, 29(2), 92–104.

National Institute of Justice. (2022). *Research on Body-Worn Cameras and Law Enforcement*. <https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement>

National Institute of Standards and Technology. (2019). *Face Recognition Vendor Test Part 3: Demographic Effects* (NISTIR 8280). <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

National Institute of Standards and Technology. (2026). *Face Recognition Technology Evaluation: Demographic Effects in Face Recognition*. https://pages.nist.gov/frvt/html/frvt_demographics.html

National Research Council. (2009). *Strengthening forensic science in the United States: A path forward*. National Academies Press. <https://nap.nationalacademies.org/catalog/12589/strengthening-forensic-science-in-the-united-states-a-path-forward>