

How Technology Has Contributed To The Problems In Criminal Justice

Posted on October 14, 2019

Introduction

The speed of technological change is accelerating, and criminal justice agencies are regularly offered tools that promise faster investigations, improved officer safety, more accurate identification, better prediction, and greater public accountability. The original essay correctly approaches these promises with caution. Technology is never simply an isolated device; it enters institutions that already contain laws, incentives, professional cultures, inequalities, data limitations, and political pressures. A camera may record an encounter without determining how the footage is interpreted. A DNA database may help identify an offender while also retaining information about innocent relatives. A predictive system may allocate police attention according to past crime data, even when those records reflect earlier patterns of enforcement rather than the complete distribution of harmful behavior. The central problem is therefore not whether criminal justice should accept or reject technology as a whole. It is how policymakers can decide which tools serve legitimate goals, which produce unacceptable costs, and which require testing, limitation, or abandonment. (Lanier & Cooper, 2016)

The title asks how technology has contributed to problems in criminal justice, but the original discussion does not claim that technology is inherently harmful. It argues that new tools are often adopted before their effects are properly established. Financial cost, privacy loss, biased data, weak evaluation, vendor secrecy, and institutional enthusiasm may create consequences that were not included in the sales proposal. At the same time, well-designed technology can preserve evidence, increase access to information, support transparency, and reduce certain forms of error. A serious analysis must therefore connect each technology with the specific problem it is expected to solve and evaluate both intended and unintended outcomes. (Lanier & Cooper, 2016)

How Do Policymakers Construct an Improved System? Is There an Application?

A growing range of tools is available to law enforcement and other criminal justice institutions, including body-worn cameras, automated license-plate readers, gunshot-detection systems, DNA analysis, facial recognition, digital forensics, drones, risk-assessment software, electronic monitoring, and predictive analytics. The original essay asks how policymakers should move forward when many of these tools are insufficiently confirmed and carry financial and confidentiality costs. The first requirement is to define the goal before selecting the application. A department should state whether

it is attempting to reduce violent crime, improve evidence collection, protect officers, reduce unnecessary detention, strengthen public trust, locate missing people, or improve case processing. Without a clear goal, agencies may measure what the technology easily produces rather than what the public actually values. (National Institute of Justice, 2026)

For example, a body-camera program can report the number of devices purchased, hours recorded, and files uploaded. Those figures show activity but not success. Success may instead involve changes in complaint resolution, use of force, evidentiary quality, officer behavior, public confidence, or the fairness of encounters. Similarly, predictive-policing software may generate maps and risk scores, but the number of predictions does not establish that crime declined or that police resources were allocated fairly. The original essay's distinction between easy metrics and meaningful outcomes is therefore essential. Policymakers should specify the outcome, establish a comparison method, collect baseline data, and decide in advance what evidence would justify expansion, modification, or termination. (National Institute of Justice, 2021; National Institute of Justice, 2026)

An improved system also requires independent evaluation rather than relying only on a vendor or the agency that purchased the product. NIJ's research portfolio emphasizes testing and evaluation because effects vary by implementation, policy, training, and local context. A tool that appears effective in one department may not transfer to another with different staffing, crime patterns, community relationships, or data systems. Pilot programs should include clear rules, technical validation, legal review, community consultation, cost analysis, and public reporting. Where possible, randomized or strong quasi-experimental designs should compare outcomes with a credible alternative. Evaluation should also examine unequal effects across neighborhoods and demographic groups rather than reporting only an average. (National Institute of Justice, 2026)

Body-Worn Cameras

The original essay uses cameras as its main example and notes that simply counting uploaded video is much easier than assessing effects on police misconduct or community trust. Body-worn cameras illustrate both the promise and the limitations of criminal justice technology. They can preserve an audiovisual record, support investigation, help review complaints, provide training material, and sometimes influence behavior during encounters. Yet the evidence is mixed across studies. Some evaluations have found reductions in complaints or use-of-force reports, while others have found limited or no statistically significant effects on major outcomes. Results depend on activation rules, officer discretion, supervisory review, public awareness, and the consequences attached to recorded misconduct. (National Institute of Justice, 2021)

A camera does not capture every relevant fact. Its field of view differs from the officer's perception, and important events may occur before activation, outside the frame, or in poor lighting and sound. Footage can appear objective while still requiring interpretation. Viewers know the outcome and may evaluate earlier behavior with hindsight. Camera position can also affect judgments about threat and

intention. Agencies therefore need policies for activation, notice, access, retention, redaction, evidentiary use, release to the public, and recording in homes, hospitals, schools, and encounters with victims. Failure to establish these rules can convert a transparency tool into a new system of surveillance. (National Institute of Justice, 2021)

The original essay compares cameras with training on implicit bias and suggests that training might sometimes achieve a similar reduction in misconduct at lower cost. The precise comparison requires evidence, because one intervention does not automatically substitute for the other. The broader point is sound: policymakers should compare the proposed technology with less expensive or less intrusive alternatives. Improved supervision, de-escalation training, staffing, procedural-justice practices, disciplinary consistency, and community-based violence prevention may address the goal more directly than purchasing devices. Technology should be evaluated against the best available alternative, not against doing nothing. (National Institute of Justice, 2021)

Facial Recognition and Identification Error

Facial recognition extends the concern about easily generated outputs. A system can return a ranked list of candidate images within seconds, but that result is not an identification by itself. Accuracy depends on the algorithm, image quality, database composition, threshold settings, and operational procedures. NIST evaluations have documented demographic differentials in many face-recognition algorithms and have shown that poor-quality images can substantially affect performance. These findings do not mean that every algorithm fails in the same way or that the technology can never be used. They mean that policymakers must understand the specific system's tested performance under conditions resembling actual deployment. (National Institute of Standards and Technology, 2019; National Institute of Standards and Technology, 2026)

The greatest criminal justice risk occurs when an algorithmic lead is treated as conclusive evidence. A false candidate may shape an investigation, influence witnesses, or lead officers to interpret later evidence in a confirmatory manner. Safeguards should require trained human review, documentation of image quality and search parameters, disclosure to prosecutors and defense counsel, and independent corroboration before arrest. Databases also require scrutiny. Searching driver's-license, passport, mugshot, or private-image collections raises different legal and ethical issues, particularly when individuals never consented to criminal investigative use. The system's speed does not remove the need for probable cause, evidentiary reliability, and procedural fairness. (National Institute of Standards and Technology, 2019)

Predictive Policing and Historical Data

The original essay discusses technologies that direct police resources according to previous crime patterns. These tools may forecast locations, times, or individuals considered at elevated risk. The

central difficulty is that recorded crime data are not a neutral map of all crime. They reflect where police were deployed, which behavior was visible, who reported offenses, whose reports were taken seriously, and which incidents led to records. If officers repeatedly patrol one neighborhood, they may detect more low-level offenses there, creating additional data that directs future patrol back to the same area. This feedback loop can make enforcement intensity appear to confirm the model's prediction. (Lanier & Cooper, 2016)

Prediction is also not prevention. A system may correctly estimate that incidents are more likely in a location without identifying which intervention would reduce harm. Saturated enforcement may increase stops and arrests without addressing the conditions producing violence. A different response—lighting, youth services, conflict mediation, environmental design, or focused investigation of a small number of serious actors—may produce better outcomes. Policymakers should therefore separate forecasting accuracy from policy effectiveness. The relevant question is not merely whether the model predicts a recorded event, but whether acting on the prediction produces a lawful, equitable, and measurable public benefit. (National Institute of Justice, 2026)

DNA Analysis and Expanding Databases

DNA technology has transformed criminal investigation by linking biological evidence to suspects, excluding innocent people, identifying remains, and supporting post-conviction review. It can correct error as well as assist prosecution. Problems arise when the scientific power of DNA encourages overconfidence or when databases expand without adequate governance. Laboratory contamination, sample mixtures, transfer, degradation, interpretation of complex profiles, and misleading statistical presentation can affect conclusions. DNA presence also does not always establish when or how material was deposited. (National Research Council, 2009)

Database policy raises further questions. Retaining profiles from convicted people, arrestees, victims, elimination samples, or relatives involves different justifications. Investigative genetic genealogy can identify potential relatives through consumer or public genealogical data, extending investigation to people who never provided DNA to law enforcement. Such methods may be valuable in serious unsolved cases, but they require rules on eligible offenses, warrants or legal process, informed consent, vendor access, family privacy, data deletion, and confirmation. A powerful technology needs stronger procedural safeguards, not weaker ones. (National Research Council, 2009)

Digital Evidence and Information Overload

Modern cases may involve phones, cloud accounts, social media, vehicle systems, home cameras, location records, and encrypted communications. Digital evidence can reconstruct timelines and relationships, but its volume creates practical problems. Agencies need trained examiners, secure storage, validated tools, chain-of-custody procedures, and methods for separating relevant

information from private material unrelated to the investigation. Backlogs may delay cases, while broad extraction can expose years of a person's communications, photographs, health information, and associations. (National Institute of Justice, 2026)

The meaning of digital data also requires interpretation. A location point has a margin of error; an account may be shared or compromised; a message may be ironic, quoted, or removed from context. Deleted data do not automatically prove consciousness of guilt. Courts and investigators must distinguish technical possibility from evidentiary inference. Vendor tools should be tested and their limitations disclosed. When software produces a report that no one in the agency can independently explain, meaningful challenge becomes difficult. (National Institute of Justice, 2026)

Political Challenges

The original essay recognizes political pressure as a powerful but blunt force. Public outrage following violence or misconduct may push agencies to adopt a visible solution quickly. Cameras, detection systems, databases, and analytical platforms can signal action even before there is evidence that they address the underlying problem. Private vendors also shape the policy environment through demonstrations, grants, lobbying, and claims of innovation. Once a department invests in infrastructure, training, contracts, and data integration, abandoning an ineffective tool becomes politically and financially difficult. (Lanier & Cooper, 2016)

Local advocates may reasonably demand technology that appears to offer accountability or safety, but one department's decision does not establish a national best practice. Communities differ in law, history, resources, and trust. Policymakers should communicate uncertainty honestly rather than presenting pilot technology as proven. Procurement documents, validation studies, error rates, contracts, data-sharing terms, and evaluation reports should be available for public scrutiny unless a specific security need justifies limited withholding. Secrecy can prevent residents, researchers, journalists, defense lawyers, and elected officials from examining whether the tool functions as claimed. (National Institute of Justice, 2026)

Political challenges also arise from unequal participation. Communities most affected by surveillance may have the least influence over procurement. Consultation held after a contract is signed cannot shape the fundamental decision. Meaningful governance involves early notice, accessible explanation, opportunity to question technical claims, and representation from affected neighborhoods, civil-rights organizations, practitioners, technologists, and defense as well as prosecution. Public participation does not replace expert testing, but it identifies values and risks that a performance benchmark may overlook. (Lanier & Cooper, 2016)

Privacy, Confidentiality, and Data Governance

The original essay mentions confidentiality costs, which have grown as systems collect more persistent and linkable data. A single camera file, license-plate scan, face template, location record, or risk score may appear limited, but combining databases can create detailed patterns of movement and association. Retention increases the possibility of breach, misuse, unauthorized search, and secondary use beyond the original purpose. Agencies need rules that define what is collected, why it is needed, who can access it, how use is audited, when it is deleted, and whether it can be shared with other government bodies or private companies. (Lanier & Cooper, 2016)

Data minimization is an important principle: a system should collect only what is necessary for a legitimate objective. Audit logs should record access, and violations should have consequences. Accuracy and correction procedures are also essential because an incorrect label or association may follow a person across systems. People may never know that inaccurate data influenced a stop, bail recommendation, supervision condition, or investigative priority. Due process requires pathways for disclosure and challenge when technology materially affects liberty. (National Institute of Justice, 2026)

How Technology Can Contribute to Mass Confinement

Technology is often presented as an alternative to incarceration, but it can widen the number of people under supervision. Electronic monitoring, automated reminders, drug-testing systems, and risk scores may allow some people to remain in the community, yet they can also impose new conditions on individuals who previously would have received less intensive supervision. Technical violations, device failures, charging problems, inaccurate location alerts, or inability to pay fees may lead to sanctions unrelated to new criminal harm. (Lanier & Cooper, 2016)

Risk-assessment instruments can support consistency, but they are built from selected variables and historical outcomes. If past outcomes reflect unequal policing, prosecution, employment, housing, or access to treatment, the model may reproduce those patterns. A score should not replace individualized judgment, and the person affected should be able to understand and contest the information used. Policymakers must examine whether a tool truly reduces detention and imprisonment or merely creates a digital extension of confinement. (National Institute of Justice, 2026)

Principles for Responsible Adoption

The original essay calls for clear aims, research, and severe assessment. Those principles can be

developed into a practical sequence. First, define the public problem and the rights that may be affected. Second, compare technological and non-technological alternatives. Third, validate the tool under realistic conditions and disclose error rates and limitations. Fourth, establish legal authority, procurement safeguards, privacy rules, training, and accountability before deployment. Fifth, conduct a limited pilot with an independent evaluation and predefined outcomes. Sixth, examine differential effects across demographic groups and neighborhoods. Finally, create a sunset or review mechanism so that continued use requires evidence rather than institutional inertia. (National Institute of Justice, 2026)

Human oversight must also be meaningful. It is not enough to place a person at the end of an automated process if that person lacks time, expertise, authority, or access to challenge the output. Staff should understand what the system measures and what it cannot establish. Records should show when technology influenced a decision. Prosecutors should meet disclosure obligations, defense lawyers should be able to examine relevant methods, and courts should evaluate reliability rather than assuming that computerized output is objective. (National Research Council, 2009)

Conclusion

The effects of [criminal justice technology](#) vary across tools, agencies, and implementation settings. Body-worn cameras, DNA analysis, facial recognition, predictive systems, digital forensics, and electronic monitoring can each provide genuine benefits, but none is self-justifying. Technology has contributed to criminal justice problems when agencies adopted it without clear aims, treated activity metrics as outcomes, relied on biased or incomplete data, accepted vendor secrecy, expanded surveillance, or failed to evaluate alternatives. (Lanier & Cooper, 2016; National Institute of Justice, 2026)

Being open to innovation should therefore be combined with skepticism toward any agency or company that resists rigorous assessment. The correct goal is not to collect the most data or deploy the newest application. It is to produce safer communities, fairer procedures, reliable evidence, appropriate limits on state power, and greater public confidence. Technology should remain a means to those ends. When the tool becomes the policy itself, criminal justice risks measuring technological activity while losing sight of justice. (National Institute of Justice, 2026)

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. (2021). *Research on body-worn cameras and law enforcement*.

National Institute of Justice. (2026). *Technology research and development portfolio*.

National Institute of Standards and Technology. (2019). *Face Recognition Vendor Test Part 3: Demographic effects* (NISTIR 8280).

National Institute of Standards and Technology. (2026). *Face Recognition Technology Evaluation: Demographic effects*.

National Research Council. (2009). *Strengthening forensic science in the United States: A path forward*. National Academies Press.