Technology Before, During, and After Incarceration: Current Product Landscape, Sociotechnical Concerns, and Legal Considerations in the U.S. Context

YAEL EIGER, Allen School of Computer Science & Engineering, University of Washington, USA
TAYLOR HANSEN, Allen School of Computer Science & Engineering, University of Washington, USA
TEANNA BARRETT, Allen School of Computer Science & Engineering, University of Washington, USA
JEVAN HUTSON, School of Law, University of Washington, USA
BRYCE CLAYTON NEWELL, School of Journalism and Communication, University of Oregon, USA
FRANZISKA ROESNER, Allen School of Computer Science & Engineering, University of Washington, USA

Emerging technology, including AI, is proliferating throughout the U.S. carceral system. These technologies are marketed to prisons and police departments and then procured using taxpayer money. Previous investigative reporting has exposed troubling kickback schemes, unconstitutional data collection practices, and biased algorithmic outcomes in a handful of prominent technologies (e.g., Flock, Palantir, Clearview AI, COMPAS). In this work, we consider the broader ecosystem of carceral technologies: we catalog 122 products from 53 companies selling technology to carceral institutions. In a collaboration among computer science, law, and surveillance studies scholars, we surface sociotechnical, ethical, and legal concerns related to the use and deployment of these technologies, including concerns related to privacy, accuracy, fairness, censorship, due process, and more. We present case studies of technology advertised for deployment in three stages of the carceral cycle: before, during, and after incarceration. We call for increased transparency and auditing, more research on the impact of these technologies, and more research on the emerging legal and regulatory challenges.

ACM Reference Format:
Yael Eiger, Taylor Hansen, Teanna Barrett, Jevan Hutson, Bryce Clayton Newell, and Franziska Roesner. 2026. Technology Before, During, and After Incarceration: Current Product Landscape, Sociotechnical Concerns, and Legal Considerations in the U.S. Context. In *The 2026 ACM Conference on Fairness, Accountability, and Transparency (FAccT '26), June 25–28, 2026, Montreal, QC, Canada.* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3805689.3806473

1 Introduction

As in most areas of society, technology has increasingly permeated throughout the U.S. carceral system. Surveillance technology increasingly intersects with people's lives before they are incarcerated (e.g., policing technology), while they are incarcerated (e.g., communication surveillance), and after they are incarcerated (e.g., electronic monitoring). Technologies in this sector (as in others) also increasingly incorporate artificial intelligence [62, 124, 182]. Although carceral technologies are developed and deployed with the apparent aims of public safety, a growing body of academic literature and investigative journalism has raised concerns about the often problematic impacts

Authors' Contact Information: Yael Eiger, Allen School of Computer Science & Engineering, University of Washington, Seattle, USA; Taylor Hansen, Allen School of Computer Science & Engineering, University of Washington, Seattle, USA; Teanna Barrett, Allen School of Computer Science & Engineering, University of Washington, Seattle, USA; Jevan Hutson, School of Law, University of Washington, Seattle, USA; Bryce Clayton Newell, School of Journalism and Communication, University of Oregon, Eugene, USA; Franziska Roesner, Allen School of Computer Science & Engineering, University of Washington, Seattle, USA.

FAccT '26, Montreal, QC, Canada

ACM ISBN 979-8-4007-2596-8/2026/06
https://doi.org/10.1145/3805689.3806473

of these technologies on currently or formerly incarcerated people, their loved ones, other marginalized populations, and the general public. For example, prior work has documented how mass surveillance technology disproportionately targets non-white residents [85, 95, 119] exhibits racial and gender biases [47, 66, 101, 182], chills speech of currently incarcerated people and their loved ones [38, 148], and introduces new risks for people who are forced to accept court-mandated electronic monitoring [147, 197].

In this work, we explore the broader landscape of carceral technology in the U.S. These technologies (including products, services, and infrastructure) are generally created and sold by for-profit companies [22, 39, 94, 117, 158] and acquired by carceral institutions (including police and prisons) with taxpayer dollars. The public rarely has insight into these companies and products purchased with taxpayer funds, and the limited information available from existing journalism and research has exposed substantial risks of privacy, censorship, and bias. We ask:

RQ1: What is the **current landscape** of technology products advertised to carceral institutions in the U.S.?

To answer this question, we collected, qualitatively coded, and cataloged the offerings from a large set of carceral technology vendors. These vendors (N=53) advertised at the U.S.'s largest annual carceral technology expo, the American Correctional Association (ACA)'s Annual Congress, which one of the authors attended in September 2025. The ACA "[champions] the cause of corrections and correctional effectiveness" [33], and its biannual conferences provide opportunities for vendors to advertise to "corrections officials from the county, state and federal levels, as well as from probation and parole and community corrections agencies" [32]. Based on the vendor booths at the September 2025 Congress and their online offerings, we identified 122 products and classified them into 11 different product types, spanning the carceral cycle (before, during, and after incarceration).

RQ2: What sociotechnical and policy **concerns** arise from the deployment of these technologies?

After describing the product ecosystem, we dive into six case studies and present both sociotechnical and legal concerns/risks which arise from their use. This set of concerns is the result of a crossdisciplinary collaboration spanning computer security and privacy (three authors), surveillance studies (one author), HCI (one author), and law (two authors). We explore these technologies from the perspectives not of the immediate buyers (i.e., police and prisons) but of their targets (i.e., currently or formerly incarcerated people, or in some cases the general public). These concerns include technical issues like computer security and privacy risks, AI-related risks like fairness, bias, and hallucination, as well as legal, policy, and ethical concerns like due process and constitutionality. Overall, this paper contributes to a growing conversation around potential harms from carceral technologies in the U.S., revealing a wide landscape of technologies developed for use throughout the carceral cycle that raise numerous technology and policy concerns. Our work points to areas where further academic, legal, and public scrutiny is needed, especially as these technologies increasingly incorporate AI.

2 Background and Motivation

Over the last two decades, public outcry has exposed the harms of private, for-profit prisons in the United States [26, 31, 92, 108, 176, 188]. But whether a prison is publicly or privately operated, it is filled with products, technology, services, and infrastructure marketed by for-profit companies [22, 39, 94, 117, 127, 158, 168], which prisons procure and contract using taxpayer dollars. The non-profit Worth Rises [158, 159] details how "more than half of the $80 billion spent annually on incarceration by government agencies is used to pay the thousands of vendors that serve the criminal legal system."

These companies showcase and advertise their products to prison and police officials at trade shows, expos, and conferences around the nation [168, 183]. The oldest and largest of such gatherings is the ACA annual conference [93, 183, 184]. One factsheet describes how the ACA "boast[s] that 81 percent of corrections industry sales

are made at trade shows" like theirs. These organizational trade shows and conferences have themselves been investigated for the murky relationships between the companies paying to participate are the same organizations that, in turn, set policy and guidelines for the operations of thousands of U.S. prisons [184].

Previous research and investigative reporting has detailed how some well-known technologies in this space — e.g., Amazon Ring cameras, Palantir data mining, BI SmartLink electronic monitoring, Flock policing technologies — cause, amplify, and facilitate various harms, including opaque data sharing practices with government entities and other companies [54, 79, 84, 88, 124, 178], warrantless surveillance [53, 79, 110], and the use of biased AI models which amplify biased policing practices [43, 67, 85, 88, 95, 101, 116, 119, 123].

While previous work has investigated individual companies or technologies, we see the need for a broader view of this ecosystem and the concerns the technologies raise, inspired by the ecosystem-focused view of those articulating the Prison Industrial Complex [39, 55–58, 75, 76]. This assessment is particularly crucial at the present moment, when AI (including "generative" and "agentic" AI) has begun to proliferate through every industry.

We consider technologies in a three-part carceral cycle: technology used **before** someone is incarcerated (e.g., technology used by police to find, produce evidence about, and generate evidence to arrest and incarcerate); technology used **while** someone is incarcerated (e.g., to surveil an incarcerated person's communications with loved ones and lawyers); and technology used **after** someone is incarcerated (e.g., electronic monitoring). These lines can be blurry, as surveillance technologies are becoming ubiquitous in every phase of the carceral cycle and in the "free world", including in luxury and consumer products [125]. The consideration of these three phases is inspired in part by Michel Foucalt's "carceral circuit" in which the three phases "support one another and form a circuit that is never interrupted" [73].

3 Methodology

Gathering Data at the ACA Congress. While attending the September 2025 ACA Congress, one author gathered advertising material, brochures, and print information from all vendor booths selling technology. Booths deemed out of scope included, for example, companies advertising food services (e.g., Aramark), healthcare (e.g., Centurion Health), and hygiene products (e.g., Colgate-Palmolive). In addition to gathering physical advertising materials, the author took photos (with permission) and wrote notes recording their impressions (e.g., when vendors offered live demos of their products). The author also attended workshops, lectures, and demonstrations, which helped provide insights into the threat model of prisons and police agencies who were presenting about their use of technology. The ACA is open to the public, and the author registered as a student; they made their student status clear to all vendors and conversation partners.

Expanding Dataset of Products. At the ACA Congress, we received pamphlets, advertising literature, and information from 53 vendor booths. Using the 53 pieces of advertising literature, we collated a list of vendors and surveyed each company's technology product offerings by using online searches and gray literature review, indexing a total of 122 products.

Classifying Product Types. We classified the 122 products into 11 different product types, described in Table 1. One initial author qualitatively coded the products according to several axes: the technology's use case, how it works, who is the expected user, and who is the expected subject. Through iterative discussion with other authors, this codebook and its application was refined, resulting in 11 categories of technology with distinct purposes, users, and subjects.

Surfacing Concerns. Our team includes computer security and privacy researchers, legal experts, technology policy and ethics researchers, and surveillance studies scholars. Through iterative discussion, we surfaced and refined a set of sociotechnical, ethical, and legal concerns about the products in our catalog.

Table 1. This table identifies the types of products in our catalog based on which part of the carceral cycle they are marketed for, and on the intended targets and end users. Italicized "targets" indicate whether the target includes non-incarcerated people (e.g., the general public or communication partners of incarcerated people). Colored in gray are the categories of technologies which are in our codebook but which we do not discuss further as case studies in this paper. Colored in pink are the "before incarceration" (Section 5) case studies; in blue are "during incarceration" (Section 6); in green are "after incarceration" (Section 7).

Category	Section	Before	During	After	Use Cases	Target	User
Policing Tech	5.1	✓			To assist the police	*Everyone*	Police
Sentencing Algorithms	5.2	✓			To predict outcomes for criminal sentencing	*People accused of a crime*	Judges
Chatbot Assessments	6.1		✓		To assess or find information for placement of an incarcerated person	Incarcerated people	Prison staff
Communication Surveillance	6.2		✓		To surveil incarcerated people and their messages	Incarcerated people and *the people they talk to*	Prison staff
Counter-Drone	6.3		✓		To detect unwanted drones in prison airspace	*Drone pilots*	Prison staff, police officers, military
Electronic Monitoring	7.1			✓	To monitor someone released from prison into "community custody" or awaiting trial	*Formerly incarcerated people; people awaiting trial or immigration hearings*	A "community custody officer" in most cases
Prison Monitoring			✓		To surveil carceral facilities (e.g., CCTV)	Incarcerated people and *visitors to carceral facility*	Police and prison staff
Contraband Detection			✓		Scanners (physical or network) to detect unwanted objects	Incarcerated people and *visitors to carceral facility*	Prison staff
Tech for Incarcerated People			✓		To communicate with people on the outside world, also to consume media and education	Incarcerated people	Incarcerated people
Infrastructure Support			✓		To build prison hardware and network infrastructure	-	Prisons
Data Aggregation Software		✓	✓	✓	To coalesce, manage, and analyze policing or incarceration information from a variety of sources	*Everyone*	Police, prison staff, parole officers, etc.

Limitations. A number of well-known products that are sold to prisons and police agencies do not appear in our dataset because they were not vendors at the ACA Congress — e.g., companies like Flock, Clearview AI, Palantir, BI SmartLink, Convenant Eyes, Accountable2You. These companies and others have already been the topic of prominent investigative reporting [54, 61, 113, 164]. If those companies had been present at the ACA, their products would be included in the categories we developed, suggesting that our taxonomy is comprehensive. For example, Flock would be categorized alongside their competitor in policing technology, Axon; BI SmartLink would be categorized with their competitor in electronic monitoring, Buddi. We believe that the omission of these companies caused no substantial change in our codebook, catalog, or set of sociotechnical and legal concerns — particularly since the associated concerns have already been widely discussed in the popular press. If there are other companies that were not present at the ACA, and which would have substantially changed our findings, they are unknown to us.

Moreover, we emphasize that our research is qualitative: our dataset is not intended to be a comprehensive listing of all companies or technologies in this space, but rather a mechanism to surface the *types* of technologies

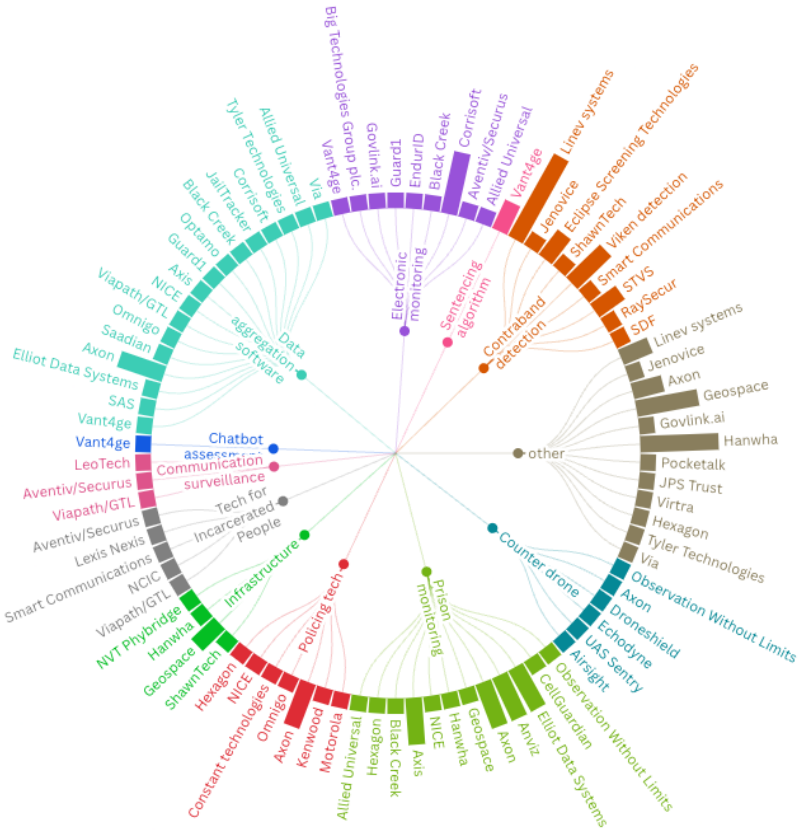

Fig. 1. A radial diagram depicting the types of technologies in the carceral system and the companies involved. The height of the bar denotes the relative number of *products* that the company markets in the category.

being marketed, and their potential impacts. We believe that the 122 products from the 53 ACA vendors — and the resultant concerns — bring important attention to a wide range of potential harms with carceral technologies (many previously not substantially discussed in research) in the U.S.

4 Carceral Technology Ecosystem Overview

We begin by providing an overview of the technologies advertised at the 2025 ACA Congress. Our classification of products resulted in 11 categories, summarized in Table 1. We also highlight whether each technology category also targets non-incarcerated people (e.g., the general public or communication partners of incarcerated people); this fact may be important in the legal context because non-incarcerated people retain certain privacy and legal rights that may be limited for incarcarated people.

The radial diagram in Figure 1 maps these product categories to the companies that provide them. A large number of companies are involved in this ecosystem; though a few are large and prominent (like Axon), many others are not widely known or discussed. Some are prominent outside of the carceral ecosystem (e.g., Motorola) but have a few individual product offerings in this space. Our investigation revealed that these companies are mostly independent from each other, without formal ownership/subsidiary relationships.

Next, we dive into case studies of several product categories: before (Section 5), during (Section 6), and after (Section 7) incarceration. Table 1 provides section references for each product category. We chose these case

studies for several reasons: to provide coverage of phases of the carceral cycle and types of concerns, our collective assessment of novelty (including the growing use of AI), and/or the gravity of potential harms.

5 Before Incarceration: Policing and Sentencing Technologies

We now turn to our case studies. In each subsection, we summarize the technologies currently advertised by companies in this space and then discuss potential harms and technical, legal, and ethical concerns.

5.1 Policing Technology

The carceral cycle begins with technologies used by law enforcement to surveil, monitor, investigate, aggregate, and report data about people. These technologies and use cases are broad, including automated license plate readers, police body cameras, dispatch software, digital evidence aggregation, and analysis software. The dominant player in this ecosystem is Axon (see Figure 1), formerly known as TASER International.

AI is becoming a key feature (or at least a key point for advertising) in many of these products. For example, Axon recently announced its "AI Era Plan" [37]. This includes detection and recognition tools, transcription and translation services, and tools like Axon's Draft One, a tool that uses Open AI's GPT-4 Turbo to transcribe police body camera footage and assist officers in writing police reports [114], or Fusus, their "real-time operations" software that allows police agencies to unify data across the Axon product suite (e.g., surveillance cameras, body cameras, ALPRs, 911 dispatch data, etc) and to analyze this data (increasingly with the support of AI) [37, 124].

5.1.1 Sociotechnical Concerns. There is an extensive body of research into the racialized, unequal, and problematic uses of technology in U.S. policing [39, 40, 43, 44, 64, 66, 105]. The expansion of technology in this space amplifies these harms and creates new sources of concern, such as bias and hallucination from generative AI. The results can be severe: someone can become the victim of false arrest, confinement, prosecution, and resultant trauma.

Prior work has already documented cases of policing technologies — such as facial recognition — introducing or amplifying existing **bias**. There have been cases of false arrest and imprisonment due to facial recognition misidentification, and the rates of misidentification are 10 to 100 times higher for people of color than for white people [39, 47, 49, 66, 133, 150, 180, 182, 194]. Inioluwa Deborah Raji, Timnit Gebru, and co-authors detail why eradicating bias in these systems is challenging [154]: (1) expanding training datasets to reduce bias creates privacy risks (which increase when adding more data on underrepresented groups), (2) increasing representation is often dependent on a reductive annotation of intersectional and nuanced identities, and (3) problems revealed in audits can result in companies making their models harder to audit in the future. Superficial audits can also help police and prison agencies "ethics wash" their technology to avoid public concerns [106].

With the introduction of *generative* AI into policing, such as Axon's Draft One, there are bias concerns as well as new concerns about **hallucinations or other inaccuracies** introduced by the model. While Axon states that the model they use in Draft One has the "creativity turned off," and that it uses "a model that is calibrated to prevent embellishment or speculation" [145, 175], model accuracy is an ongoing research challenge. Moreover, many concerns about bias remain in how the narrative about an incident is crafted, what information is omitted, and whose perspective is favored.

There are also serious **security and privacy** concerns when a private company is increasingly providing the tools to collect and store citizen data. Can these cameras see into private homes? How do they deal with this private information? How does a private company handle data requests from other government entities (such as I.C.E.) that may be otherwise blocked by government siloing and the need for warrants? These are also not hypothetical worries — Flock has recently attracted public scrutiny for data security failures, ranging from data leaks to password-less cameras exposed to the entire internet, and warrentless data sharing with other companies and government entities [72, 112, 177, 178, 200].

Lastly, there is a **censorship and chilling effect** as a result of surveillance. The feeling of being watched impacts the freedom of individuals to act as themselves in the outside world. Surveillance scholar Shoshana Zuboff describes this as a world with increasingly "no exit" or reprieve from being watched [103, 206]. Furthermore, as what is deemed a crime changes over time and across jurisdictions (e.g., abortion), this data collection can prove harmful in the future, even if it feels safe in the present.

5.1.2 Legal Discussion. Axon's "AI Era" policing ecosystem and the proliferation of Flock surveillance technologies are prominent examples of technologies that intensify long-running **constitutional concerns** about privatized, automated state surveillance and evidence production. The most immediate issues implicate the Fourth Amendment [171] search and seizure law. The Supreme Court has increasingly recognized that technologically augmented surveillance can create new kinds of searches even when individual data points are collected in public. *United States v. Jones* and *Carpenter v. United States* suggest that the prolonged aggregation and analysis of location data can trigger warrant requirements and heightened constitutional scrutiny [19, 21]. Axon's integrated platform approach unifying body-camera footage, ALPR outputs, real-time analytics, and AI-driven search pushes toward precisely this kind of "mosaic" surveillance.

AI-driven report writing tools (e.g., Draft One) promise to make the tedious and time-consuming task of writing incident reports more efficient, but they raise distinct **evidentiary and procedural concerns**. These expand on preexisting issues regarding the impact of officers referring to police body-camera footage when writing reports [46]. When AI is writing initial drafts based on automated interpretation of police body-camera video, defense attorneys and judges will be forced to ask whether the "underlying facts are reliable" enough for decisions that may impact a person's liberty [69]. Even if officers "review and edit," an AI-first narrative risks anchoring bias in official records and may embed unexplainable model errors into documents that later shape probable cause determinations, charging decisions, plea bargaining, and trial credibility assessments [51, 99]. The fact that AI drafted much of a report distorts the legal determination about the reliability of the report [69]. Two US states have already regulated the use of AI report writing tools by requiring some form of disclosure and, in California, to produce an audit trail [68].

Misidentification and over-targeting risks may become actionable when agencies adopt tools known to produce racially disparate outcomes without adequate validation, training, or oversight [47, 155], implicating **due process and equal protection concerns**. While doctrinal hurdles remain for proving discriminatory intent, civil rights frameworks increasingly treat predictable disparate harms from automated enforcement as a governance failure that merits judicial and legislative intervention [155].

Finally, the spread of public-private surveillance arrangements puts pressure on **accountability** norms. When a single vendor supplies the capture, storage, analysis, and redaction stack, the risk is not just constitutional overreach but institutional dependency — where democratic oversight becomes contingent on a contractor's architecture choices, pricing, and disclosure posture [99]. The legal system's challenge to these forms of "platform policing" [74, 202] is to reassert constitutional and public law constraints on an end-to-end corporate policing infrastructure. The above risks are magnified by **trade secrecy and contracting practices** that can limit defense access to system design, error rates, or audit materials, complicating discovery and undermining meaningful adversarial testing [99].

Policing Technology Takeaways:

- These systems can amplify existing bias, and cause legal evidentiary concerns. But these problems also create a potential path for challenging its usage.
- Privatization and "platform policing" hinder accountability and democratic oversight.

5.2 Sentencing Algorithms

Technology is also used in sentencing and "risk assessment", to determine the punishment of a person who has been convicted of a crime. The use and potential harms of algorithms in sentencing have received attention in popular media and in academic research, particularly through coverage of the COMPAS algorithm [34, 71, 78, 151, 204]. Our taxonomy surfaced two other sentencing algorithms, both made by the company Vant4ge: M-PACT and STRONG-R. STRONG-R is for adult assessment, while M-PACT is specifically for youth. M-PACT aims to assess a youth's risk factors across 12 domains: "aggression, alcohol and drugs, attitudes/behavior, criminal history, employment, family, living arrangements, mental health, relationships, school, skills, and use of free time." Vant4ge evens sells a "Prevention M-PACT" to identify youth at risk of *future* criminality.

5.2.1 Sociotechnical Concerns. These sentencing algorithms provoke major **bias, transparency, and security/privacy concerns**. Many previous discussions of bias revolve around the COMPAS sentencing algorithm, particularly its bias in falsely predicting that Black people are more likely to reoffend than white people [34, 71, 78, 151, 204]. Okidegbe [143] highlights that the risks of racialized bias are two-fold. Most directly, racialized bias results in "inaccurate and inflated predictions of riskiness" for racially marginalized individuals. But even if sentencing algorithms accurately reflect differences in risk, they reproduce racial stratification; e.g. "the factors that elevate a person's risk of engaging in violent conduct — such as poverty, pollution, unclean water, housing, and employment instability — are the very conditions that Black and other politically oppressed communities are disproportionately forced to live in" [143]. Moreover, sentencing algorithms fail to consider the possibility of rectifying these "risks" of recidivism and non-compliance if a detainee is given access to a social assistance program, community support, or a lawyer. They also do not take into account the harm of incarceration on the family and community of the person, which further contributes to the carceral cycle [142].

Okidegbe also criticizes the argument sometimes made that algorithms provide more transparency than (biased) human decisions, which would be made by judges without the use of sentencing algorithms. Unfortunately, the privatization of the technology, and the reluctance of the private companies to disclose the workings of the algorithm lead in practice to a **lack of transparency**. Some have investigated the data being ingested by sentencing algorithms and explored how it is largely or solely made up of criminal data that is itself biased and skewed. Richardson, Schultz, and Crawford refer to this as **"dirty data"** created by "dirty policing" [142, 155].

Finally, these sentencing algorithms pose potential **security and privacy risks**: they demand that detainees supply identifying, personal, and sensitive information to a court, mediated through a private company. How is this data protected? Who has access to a person's records? And what accountability measures are in place to ensure the company is adequately protecting people's data?

5.2.2 Legal Discussion. Courts have fielded challenges to the accuracy and reliability of algorithmic tools used in criminal sentencing and parole decisions [23–25, 143]. Risk assessment tools like COMPAS, STRONG-R, and M-PACT raise a stable cluster of **constitutional and administrative law problems**. The leading doctrinal flashpoint remains **procedural due process**. In *State v. Loomis*, the Wisconsin Supreme Court permitted COMPAS use but acknowledged the dangers of opacity and required cautionary limits [25]. *Loomis* underscores a structural tension: courts increasingly rely on proprietary scores that defendants cannot meaningfully challenge, despite the score's real influence on liberty [25, 51]. A second issue is **equal protection** and the amplification of structural racial inequality. Evidence-based sentencing is often sold as a check on human bias, yet the scholarly consensus is that these systems can import biased policing and socio-economic stratification into mathematical form [47, 82, 179]. Even "accurate" models may reproduce racial disparities because they treat race-correlated conditions (like neighborhood disadvantage) as predictors of future harm [82, 179]. This reframes the debate from a narrow technical question (error rates) to a legal-ethical one: whether the state may constitutionally rationalize unequal punishment through statistical proxies.

Third, these tools implicate **reliability and transparency of evidence**. Courts and legislatures have struggled to decide how much explainability is required when algorithmic outputs shape sentencing or parole decisions. Scholars argue that trade secrets claims undermine the legitimacy of criminal adjudication and weaken checks on arbitrary decision-making [51, 99]. Finally, **youth-specific and pre-justice** tools (like M-PACT variants) intensify these concerns. A risk-logic that reaches "upstream" can create a pipeline where social vulnerability is recoded as criminogenic risk, inviting early intervention that functions as surveillance and pre-punishment [82]. Given the high stakes, legislatures should require robust transparency, bias testing, and demonstrable non-carceral alternatives before permitting algorithmic risk scores to structure decisions about youth liberty and opportunity [82, 179].

Sentencing Algorithm Takeaways:

- Sentences based on "dirty data" and mathematical proxies for "risk" may amplify biased outcomes and limit someone's freedom to overcome already disproportionate social vulnerability.
- Privatization further hinders transparency and accountability.

6 During Incarceration: Assessment and Surveillance Technologies

6.1 Chatbot Assessments

Just as generative AI powered chatbots have become increasingly common across many industries since the launch of ChatGPT, so too have they appeared among carceral technologies. One example is Aida, created by Vant4ge. Aida is marketed as an "AI interviewing platform purpose built for corrections." Aida aims to replace human staff members conducting interviews of people who are being placed in a new (to them) prison or jail. Aida emits a feminine voice to ask questions of the person in order to inform their placement in educational or jobs programs, assign their housing, supervision requirements, sentencing, and/or parole decisions. Aida is marketed as an improvement over a real staff member to conduct these interviews because Aida "never gets tired" and "works tirelessly and independently to gather information in an unbiased listening environment" [193]. It was not clear to us whether Aida makes (or can make) these decisions automatically or what the role of a human-in-the-loop may be.

6.1.1 Sociotechnical Concerns. As in non-carceral contexts, the use of AI-powered chatbots raises concerns about **privacy**, **bias**, and **hallucination**. Here, the immediate user is an incarcerated person and, given the power dynamics, is particularly vulnerable. Aida creates **privacy risks** not only similar to consumer chatbots (of the data being collected by a company and perhaps used in further training), but also privacy risks exacerbated by the power dynamics in which the incarcerated person finds themselves. Aida collects and processes significant amounts of information from each conversation. It "records every word, detects inconsistencies, and provides complete transcripts with actionable summaries" [191]. It is unclear how — if at all — this collection and use of data through Aida is communicated with or consented to by the people it is used to question.

Moreover, Aida claims to be more effective than a human at extracting information. A Vant4ge whitepaper submitted for publication in the Journal of Offender Rehabilitation [192] states that incarcerated people "open up" to a greater degree when speaking to Aida, because "in correctional

Fig. 2. Aida's "privacy" booth at the ACA conference.

environments — where distrust of authority figures is common, and where many have experienced trauma or abuse while housed in institutions — AI's neutrality becomes a critical strength." While these properties can be benefits when they really lead to better outcomes (e.g., mental health support or placement) for incarcerated people, they also allow for the collection of more, potentially sensitive, information that may not always be used in anticipated or desired ways.

Bias concerns also arise. For example, Aida runs "veracity checks" to "assess the consistency of an individual's responses with known data" [190]. Where does the known data come from? How does Aida make assessments about veracity? And when Aida makes or recommends decisions impacting an incarcerated person, what information is taken into account and what kinds of (e.g., racial) bias may be incorporated? No information is provided about which models Aida uses or its overall design to allow for the transparent auditing of bias or other risks.

Another type of prediction that Aida makes, and could make in a biased way, is to flag potential risk of suicide, self-harm, or violence [192]. While addressing such risks is desirable, in practice, the way they are addressed may be harmful. Mental health support for incarcerated people is severely lacking in the U.S. [89, 139, 195]. Moreover, the divulsion or display of mental illness, including suicidal ideation and self harm risk, often leads to an extended period in solitary confinement, extreme isolation measures, a series of infractions, and other punitive outcomes for incarcerated people [45, 52, 89, 96, 152, 163, 170, 198]. This cycle is further perpetuated by the risks of suicide and self-harm that come from solitary confinement and being in prison generally [102, 146, 181, 205].

Finally, chatbot raise a concern — particularly potent in the carceral context — of **dehumanization**. At the ACA conference, the Aida demos were inside of "correctional grade privacy booths" created by the companies Duramate, iT1, and SPACEWORK, which consisted of a single chair inside of a see-through container that barely allowed an adult to stand up straight (see Figure 2) –– a far cry from the experience of talking to another person. Ultimately, the offloading of important, vulnerable, and potentially humanizing conversations to a machine risks further dehumanizing both the people who are being assessed and the prison staff, which has been found to correlate with suicidal ideation in incarcerated people [160].

6.1.2 Legal Discussion. AI-driven intake and assessment chatbots introduce a new form of custodial data extraction that sits uneasily with constitutional and statutory safeguards. The central concern is **coercion by design**. Incarcerated people face extreme power asymmetries and limited choice; "consent" to data collection is structurally compromised, making the legal framing closer to compelled institutional interrogation than to ordinary consumer chat use [8]. These systems also raise **Fifth Amendment and due process issues** when chatbot-collected statements are used to inform classification, housing, program eligibility, discipline, parole, or sentencing-related decisions. Even if the chatbot is marketed as "neutral," an AI interface that records, transcribes, and "detects inconsistencies" can function as an automated credibility assessor — a role with direct liberty consequences and little procedural transparency [8]. We note that Aida's collection practices and model choices are opaque and that the same disclosures and confidentiality protections present in therapeutic contexts (e.g., patient-client confidentiality) are absent here.

A further legal risk concerns **disability and mental health law**. If AI triage systems flag self-harm risk and trigger punitive rather than therapeutic responses (e.g., solitary confinement), this could intersect with Eighth Amendment standards around deliberate indifference and statutory disability protections requiring reasonable accommodations in carceral settings [10]. When a "safety" signal becomes a pathway to punishment, the legal legitimacy of automated mental health sorting becomes suspect.

Finally, chatbot systems extend **privatization** into intimate custodial decision-making. If vendors retain transcripts, repurpose them for product development, or share outputs across agencies, prisons may be underwriting a secondary market in vulnerable people's narratives and data. Consumer privacy statutes may offer partial

constraints, but most lack clear application to coerced custodial data flows [174]. The better doctrinal anchor may be constitutional: requiring heightened procedural safeguards and use limitations when chatbot-elicited data is used to support state action affecting liberty, safety, or family contact [8, 51]. Though many recently adopted state-level consumer data privacy laws, like the California Consumer Privacy Act (CCPA), do not explicitly address inmate data, businesses covered by those regulations regularly process "correctional consumer data" [153] when they provide private technologies to correctional facilities.

Chatbot Assessment Takeaways:

- Compelled institutional data collection compromises consent mechanisms.
- Confidentiality assurances in a "therapeutic" setting may be bypassed, despite the marketing.
- Mental health risks may be amplified by divulgence/disclosure and resultant punishment.

6.2 Communication Surveillance

Another important set of technologies in the carceral system are those that allow incarcerated people to communicate with the outside world, including messaging or speaking with their loved ones and lawyers, or accessing media or educational content. Most companies that develop communication tools for incarcerated people (e.g., Securus, Viapath) simultaneously advertise products to analyze the messages and calls taking place on them. Increasingly, this analysis is advertised as conducted by AI as opposed to previous keyword or pattern-matching techniques. For example, Securus's InvestigatorPro [166] analyzes phone calls and uses voice analysis to identify incarcerated people on calls by compiling and analyzing "a database of biometric 'voice print' data" [153] and creates a searchable database of an incarcerated person's calls. Similarly, Securus's Word Alert [167] automatically transcribes phone calls and video calls into text so that investigators can keyword search the transcript.

The company LeoTech advertises a communication surveillance tool, Verus [30, 35, 120, 121], that markets four main features: Search, Continuous Monitoring, Link Analysis, and Lexicon. Lexicon identifies slang used in the surveilled communications, because "occasionally, threats are associated with slang or code words, such as 'mosquito' for drones." Verus claims to use "the power of artificial intelligence" and (emphasis ours) "*non-biased* Natural Language Processing." How the claimed lack of bias is achieved or evaluated is not clear.

6.2.1 Sociotechnical Concerns. One concern with technology-enhanced surveillance of the communications of incarcerated people is that it is **overly broad**, e.g., capturing communications with free-world contacts. And, although incarcerated people generally lose the right to not be surveilled, the exception is in speaking with their attorneys. However, in 2015, Securus was hacked and more than 14,000 recordings of calls to lawyers protected by attorney-client privilege were leaked, revealing that these calls are still recorded by Securus [172, 173] — as well as raising **security and privacy concerns** about how data is stored and managed. Furthermore, these surveillance tools are being deployed in pre-trial jail detainment in county jails, where people are frequently held before being convicted of any crime, often because they cannot afford to pay bail [144, 196].

Similarly, there is concern around **mission/surveillance creep** or the over-collection or use of data for purposes other than those originally or publicly claimed. These concerns are not hypothetical: after Verus' initial pilot program, Reuters reported that the tool was used far beyond its purported scope. For example, conversations were flagged for containing "the Spanish word for lawyer" and for trying to expose how "detention facilities were covering up COVID-19 outbreaks" [38]. (Indeed, Verus's use to surveil communication between incarcerated people and their loved ones more generally is itself a creep of scope beyond its original stated mission to identifiable ill or sick patients during COVID-19 [38].)

Verus's identification of "slang" terms also provokes concerns around **bias** and the **criminalization of diverse speech**. There is a robustly documented history of the criminalization of Black expression and language, including

prejudice in a court or trial setting due to racist linguistic profiling [29, 42, 59, 109, 115, 122, 157, 161, 185, 186, 203]. This type of racism and linguistic prejudice has already been shown to exist in LLMs [28, 87, 130]. After Verus's deployment into New York prisons, more than 50 advocacy groups wrote a letter demanding its termination due in part to the higher error rate for Black voices. Not only will this inaccuracy produce bias, but even an accurate textual transcription of "slang" words can criminalize language out of context [38] — for instance, the Spanish word "mara" can translate as a "gang" when it also translates as "a group of friends".

6.2.2 Legal Discussion. Although it appears settled that incarcerated people can be subjected to intrusive forms of surveillance while incarcerated — and that their Fourth Amendment rights are limited in favor of granting deference to prison administrators within the boundaries of the physical prison [14] — it remains "an open question as to whether prisoners retain a privacy interest in their digital lives" [126]. As of early 2026, approximately twenty U.S. states have enacted broad consumer **data privacy laws** that could possibly be leveraged to grant incarcerated people privacy rights and impose obligations on commercial providers contracting with prisons, although their scope is limited to the consumer-business relationship, and not all businesses are subject to obligations under these laws (see, e.g., [90, 132]). Additionally, legal scholars have argued that federal regulations that allow prisons to monitor and record attorney-client communications violate incarcerated people's **rights to communicate privately with their attorneys**, as well as their **Fourth Amendment right to privacy** [60]. Widespread recording or automated analysis of privileged calls risks interference with the right to counsel and can chill defense strategy [11]. Legal scholars have argued that communication surveillance violates the **privacy rights of those held in pretrial detention** who retain a stronger presumption of innocence [97]. These individuals have a more credible argument that blanket AI-enhanced communications monitoring is disproportionate to legitimate security needs [12, 16].

The **First Amendment** also applies. Historically, the Court has required heightened scrutiny for censorship of mail and speech of incarcerated people, even while allowing security-based regulation [9, 15]. AI-driven flagging and "slang" interpretation systems risk expanding censorship through biased linguistic profiling. When "risk signals" are generated from decontextualized text, the effect is not merely surveillance but the shaping of permissible expression.

The core legal takeaway is that modern carceral communication surveillance is no longer best understood as a narrow security practice. It is a commercial intelligence pipeline whose expansion raises constitutional concerns about counsel, pretrial rights, and speech — requiring legislatures to impose explicit limits on AI transcriptions, secondary data use, and interagency sharing that go far beyond traditional prison monitoring rules [11, 51, 174].

Communication Surveillance Takeaways:

- First amendment, due process, and new data privacy laws may provide viable challenges to this surveillance, even in carceral contexts.
- This surveillance, including its overly broad scoping, risks linguistic criminalization and punishment.

6.3 Drone Detection and Disruption

Our catalog includes six companies advertising drone detection and jamming technology. There were also several workshops at the ACA Congress addressing the (claimed) growing threat of drones dropping contraband over prison walls [162]. The actual scope of the threat in practice is unclear. While there are individual anecdotal reports of such occurrences [27, 36], the Federal Bureau of Prisons reported only 479 total drone sightings in 2024 [83] — though it is unclear how many of these were indeed part of a delivery or other attack, as well as how many may have gone undetected.

The advertised technologies span drone detection, flight analysis, and drone jamming. Airsight [165], one drone-defense company, notes that jammers are illegal in the U.S. and thus focuses solely on detection. Still, other companies market jamming technology. For example, Axon markets DeDrone, a suite of "AI-powered" drone detecting and jamming technology [1]. Interestingly, another company in our taxonomy, Hexagon, makes *anti*-jamming technology to protect drones.

6.3.1 Sociotechnical Concerns. This drone detection and interception technology generates a range of concerns, including **privacy** concerns. With the deployment of radar and radio-frequency scanning, the question is: what (and who) is scooped up in this surveillance? One product, MESA echodyne [4], claims to have "no privacy impacts" while collecting information of "high evidentiary value" on drone pilots and their flying behavior — but it is unclear what privacy impacts are avoided, and how. Moreoever, we must consider **accuracy and accountability**: What are the false positive rates of contraband detection? And who is punished as a result?

6.3.2 Legal Discussion. Counter-drone systems marketed for prisons raise an underappreciated cluster of **federal preemption, communications law, and privacy issues.** The basis for most "disruption" tools — the intentional interference with drone command-and-control signals or GPS — implicates federal prohibitions on radiofrequency interference. Under the Communications Act, willful interference with licensed or authorized radio communications is generally unlawful absent specific federal authorization [7]. Federal law also prohibits the manufacture, importation, marketing, sale, or operation of unlicensed jamming technologies [3]. Thus, vendors advertising jamming technologies must obtain a federal license to even market these tools within the US. State or local prison agencies therefore face significant legal constraints if they or their vendors deploy jammer-like capabilities without clear federal approval.

Even detection-only platforms can raise **privacy issues**. RF and Remote ID monitoring may capture information about lawful hobbyists, journalists, or nearby residents. The question becomes whether persistent, automated tracking of individuals outside prison constitutes a Fourth Amendment search under the logic of technologically enhanced aggregation [19, 21]. Another issue is **evidence and accountability**. If counter-drone analytics trigger arrests or disciplinary action based on AI, defendants may need access to system error rates, detection thresholds, and audit outputs. Trade secret barriers would again collide with due process and fair trial principles [51, 99].

Finally, the **proportionality** of these systems should be legally interrogated where the alleged threat is not clearly substantiated. Where the factual predicate is weak, the legal justification for expansive airspace surveillance becomes correspondingly tenuous. The most defensible legal path likely prioritizes narrowly tailored detection, rigorous public reporting of actual contraband-drone incidence, and explicit federal authorization for any interference technology, with robust due process protections for individuals accused based on algorithmic detection systems [7, 51].

Drone Detection and Jamming Takeaways:

- Drone jamming may violate the Communications Act and other federal guidelines.
- Even detection-only systems may violate the privacy rights of unassuming citizens.

7 After Incarceration: Surveillance and Monitoring Technologies

7.1 Electronic Monitoring (EM)

After people are released from prison, often they are not free from surveillance and monitoring. A substantial set of technology in our taxonomy included electronic monitoring tools to surveil people recently released from prison and into "community custody." These tools are also used to surveil people awaiting trial, and, increasingly, migrants and immigrants in the U.S.. These tools include hardware like ankle monitors, smart watches, biometric

and alcohol monitoring devices, and software like court-mandated mobile apps. For example, Buddi makes a suite of monitoring products including the "Buddi clip & mini+", a compact and "discreet" personal tracking device with two-way voice communication"; a "smart beacon + SURETAG", a radiofrequency "curfew solution"; "ALCO TAG®", a combined GPS and transdermal alcohol monitor; and their "SMART TAG", a live tracking device aiming to provide reliable location tracking. Buddi's advertising materials state that its products include "integrated AI features to enhance monitoring" but provide no further information about the nature of the AI integration. As another example, Securus markets "Best-in-Class Monitoring" tools, as well as a "Solutions Center" to be "the de facto monitoring arm of [any] agency's electronic monitoring program." This center, located physically in Houston, TX, provides around-the-clock "electronic monitoring professionals" to law enforcement and community corrections organizations. This means that EM data is accessible not only to local government agencies but also to Securus employees in a private, third-party call center.

7.1.1 Sociotechnical Concerns. A growing body of academic literature and investigative reporting criticizes electronic monitoring [80, 111, 147, 149, 197] for reasons including **privacy**, **lack of efficacy**, and various harmful impacts to people who are monitored and their communities. On the privacy side, EM apps may collect more data, and share it with more entities, than expected or properly disclosed [147]. Moreover, prior work details the damage and toll that these monitoring programs create for subjects' mental and physical well-being, employment and housing opportunities, and more [41, 149]. At the same time, the efficacy of EM towards its stated goals is unclear: while the tools are ostensibly deployed to increase "compliance" and attendance of court hearings, there is little proof, transparency, or reporting to support these claims. For example, a government investigation of I.C.E.'s claims about their usage of electronic monitoring found that I.C.E. presents inaccurate, misleadingly-positive numbers about the benefits of EM [141]. Indeed, research shows that providing a lawyer or social assistance programs could actually be more useful for achieving the stated goals [63]. Thus, instead, EM tools effectively become a continued form of punishment for people mandated to use them [149, 197].

7.1.2 Legal Discussion. EM increasingly functions as a digital extension of incarceration. The key constitutional anchor is the **Fourth Amendment**. The Court has held that individuals on probation or parole have diminished privacy expectations, allowing suspicion-based or even suspicionless searches in some contexts [17, 18]. Yet the Court has also clarified that GPS monitoring is a search; its reasonableness depends on scope, justification, and the legal status of the person monitored [12, 20]. This matters for pretrial EM, where the presumption of innocence should constrain intrusive, continuous location tracking absent individualized necessity.

Due process concerns arise when EM data becomes the basis for revocation or reincarceration. GPS inaccuracies, geofence errors, or technology malfunctions can become alleged "violations" that trigger serious sanctions. Without robust contestation processes and technical disclosure, EM risks functioning as automated strict liability [51]. There is also the **economic and equal protection problem** of fees. Many EM programs impose costs on monitored individuals, effectively conditioning liberty on the ability to pay. This can recreate the unconstitutional dynamics of wealth-based punishment condemned in cases restricting incarceration for nonpayment [13].

Finally, the privatization layer is pivotal. The extension of monitoring to private call centers and cross-jurisdictional data sharing raises **governance concerns about accountability, security, and secondary use**. The legal reform agenda should therefore distinguish between EM used as a true alternative to detention and open-ended, AI-enhanced surveillance regimes that expand the carceral net.

Electronic Monitoring Takeaways:

- Electronic monitoring extends punishment beyond prison walls, and conditions liberty on payment.
- GPS monitoring has been legally classified as a "search" and therefore could be challenged by Fourth Amendment & due process laws.

8 Discussion and Conclusion

We have explored the ecosystem of vendors and products marketed to prisons and police agencies in the U.S., including case studies that highlight concerns about these products from sociotechnical and legal perspectives. Many of these technologies are only available and sold to law enforcement agencies and prisons, and are unavailable to researchers, auditors, activists, or accountability offices despite being paid for with public taxpayer dollars. The contracts are sometimes subject to records requests, which can take months or even years to comply with. Even if the contracts are available, we need more transparency into the technologies themselves. We cannot rely on profit-driven companies to hold themselves accountable.

Researchers and others have also noted the "ethics washing" spreading throughout the private sector [106]. We saw this in our exploration as well: for example, Axon mentions "racial bias audits" and LeoTech claims their natural language processing is "non-biased", while neither company provides enough transparency to validate these claims and the biased impacts are still seen in practice. We need independent entities, regulators, and directly impacted community collectives to run these evaluations, and that starts with having access to the actual technology: not cherry picked demos, white papers, nondisclosure agreements, and redacted contracts.

Although attempting to prevent or rectify individual harms is good (e.g., running independent audits), the most effective way to prevent harms from some technologies is to prevent their use altogether, e.g., by reducing the number of people subject to them in the first place, via restorative justice, decriminalization, and abolition. Because this paper has largely focused on the problematic nature of current and even past implementations of this technology, it is natural to feel some level of apathy, nihilism, and cynicism about the potential for change, especially when the root causes are so daunting; technosolutionism in policing is sometimes proposed in response to very real staffing shortages [118, 129], officer bias or prejudice [77, 138], police violence [100, 107], or a genuine desire for transparency and accountability [105, 131]. Technology is not the only option for mitigating these concerns, however, and alternatives are being proposed around the country. Many cities have fully unplugged and canceled their surveillance technology contracts after concerns were raised and seen [50, 65, 98, 128, 201]. Grassroots organizations all over the country have emerged to propose alternatives, and even to "watch the watchers" or conduct sousvelliance [6, 81, 86] with monitoring technology [2, 5, 91]. Beyond ceasing technological deployments, some jurisdictions have begun successful "Evidence-Based Alternatives to Policing" [156, 169, 189] for addressing gun violence [134], the school-to-prison pipeline [135], traffic safety [136], behavioral health crises [137], and have started programs to create guardrails for surveillance technology usage [48, 140]. Some progressive prisons are even attempting to prevent future crime by expanding available programming to include programs proven to (more cost-effectively) reduce recidivism (e.g., education, arts, community groups) [104, 187, 199], instead of relying on an increase in surveillance or monitoring.

At the same time, the deployment of carceral technology is encouraged by a robust, wealthy industry of private companies, lobbying organizations, and pro-surveillance policing interests. As such, the aforementioned steps in the right direction would not be possible without immense public pressure, bravery, and resistance against the status quo. Ultimately, despite the power and financial means of the companies and carceral institutions, we follow the adage of Worth Rises founder Bianca Tylek: "Powerful prison profiteers are upholding mass incarceration so they can take home billions every year, but they are not unstoppable" [70].

Acknowledgments

Thank you to the UW Security and Privacy Lab and the UW Technology Law & Public Policy Clinic. Thank you especially to Rachel Hong, Natalie Grace Brigham, Anusha Nasrulai, Kentrell Owens, Gregor Haas, Javon Hickmon, David Kohlbrenner, and Tadayoshi Kohno for feedback on early iterations. This work was done as part of the Center for Privacy and Security for Marginalized and Vulnerable Populations (PRISM), supported by the National Science Foundation under Award #2205171.

References

[1] Dedrone by Axon: Counter-Drone Defense Solutions & Systems — dedrone.com. https://www.dedrone.com/. [Accessed 23-09-2025].
[2] Deflock. https://deflock.org/.
[3] Devices which interfere with radio reception. 47 U.S.C. § 302a(b).
[4] Echodyne | High-Performance Radar for Autonomy & Security — echodyne.com. https://www.echodyne.com/. [Accessed 23-09-2025].
[5] justicecommittee. https://www.justicecommittee.org/cop-watch.
[6] sousveillance.com. https://sousveillance.com/.
[7] Willful or malicious interference. 47 U.S.C. § 333.
[8] Miranda v. Arizona. 384 U.S. 436, 1966.
[9] Procunier v. Martinez. 416 U.S. 396, 1974.
[10] Estelle v. Gamble. 429 U.S. 97, 1976.
[11] Weatherford v. Bursey. 429 U.S. 545, 1977.
[12] Bell v. Wolfish. 441 U.S. 520, 1979.
[13] Bearden v. Georgia. 461 U.S. 660, 1983.
[14] Hudson v. Palmer. *468 U.S. 517* (1984).
[15] Turner v. Safley. 482 U.S. 78, 1987.
[16] United States v. Salerno. 481 U.S. 739, 1987.
[17] United States v. Knights. 534 U.S. 112, 2001.
[18] Samson v. California. 547 U.S. 843, 2006.
[19] United States v. Jones . 565 U.S. 400, 2012.
[20] Grady v. North Carolina. 575 U.S. 306, 2015.
[21] Carpenter v. United States . 138 S. Ct. 2206, 2018.
[22] Prison Profiteers - Business Review at Berkeley, Apr. 2022.
[23] Amaker v. Schiraldi. *812 Fed.Appx. 21* (2nd Cir. 2020).
[24] Rauch v. Miniard. *2025 WL 1679515* (E.D. Mich. 2025).
[25] State v. Loomis. *371 Wis.2d 235* (Wisc. 2016).
[26] 133. Are Private Prisons in Trouble? | Brennan Center for Justice.
[27] ABC News. Drones dropping contraband into prisons fuel scams targeting Americans, Dec. 2025. https://abcnews.go.com/GMA/News/video/drones-dropping-contraband-prisons-fuel-scams-targeting-americans-128339289.
[28] Abid, A., Farooqi, M., and Zou, J. Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (New York, NY, USA, 2021), AIES '21, Association for Computing Machinery, p. 298–306.
[29] Admin, A. W. DEA and Ebonics - Society for Linguistic Anthropology — linguisticanthropology.org. https://linguisticanthropology.org/blog/2010/08/25/dea-and-ebonics/, 2010. [Accessed 18-12-2025].
[30] Admin, K. What is LeoTech? - LeoTech — leotechnologies.com. https://leotechnologies.com/news-resources/what-is-leo-technologies/, 2020. [Accessed 19-12-2025].
[31] Air, N. F. Investigation Into Private Prisons Reveals Crowding, Under-Staffing And Inmate Deaths. *NPR* (Aug. 2016).
[32] American Correctional Association. Advertising Opportunities. https://www.aca.org/conferences/advertising-opportunities.
[33] American Correctional Association. Our History & Mission. https://www.aca.org/about/history-and-mission.
[34] Angwin, J., Larson, J., Kirchner, L., , and Mattu, S. Machine Bias — propublica.org. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, 2016. [Accessed 10-11-2025].
[35] Asher-Schapiro, A., and Sherfinski, D. 'Scary and chilling': AI surveillance takes U.S. prisons by storm. https://www.reuters.com/article/world/scary-and-chilling-ai-surveillance-takes-us-prisons-by-storm-idUSKBN2I01GZ/, 2021. [Accessed 19-12-2025].
[36] Associated Press. Drone drops steak and crab legs for prisoner feast but South Carolina guards find it first, Dec. 2025. https://apnews.com/article/prison-drone-drugs-steak-crab-south-carolina-8da6576c502f2a615683b3c6d66ddae2.
[37] Axon. Axon ai era plan. https://www.axon.com/products/axon-ai-era-plan, 2025. [Accessed 30-12-2025].
[38] Barabas, C. Care as (re)capture: Data colonialism and race during times of crisis. *New Media & Society 26* (12 2024), 7351–7370.
[39] Benjamin, R. *Captivating technology: race, carceral technoscience, and liberatory imagination in everyday life*, 1 ed. Duke University Press, Durham, 2019.
[40] Benjamin, R. *Race after technology : abolitionist tools for the new Jim code*. Polity, Cambridge, UK ;, 2019 - 2019.
[41] Boe, C. S., and Rodriguez, J. Digital detention: Engagements in collaborative counter-surveillance, 2025. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/20214.
[42] Branson, D. Sounding Guilty: Criminality and Black Racialized Speech. https://d-scholarship.pitt.edu/45224/25/Branson%20-%20ETD%20-%20Final.pdf, 2023. [Accessed 18-12-2025].
[43] Brayne, S. *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press, Oxford, New York, Nov. 2020.

[44] Browne, S. *Dark Matters: On the Surveillance of Blackness.* Duke University Press, 2015.

[45] Bryant, E. The United States Criminalizes People Who Need Health Care and Housing — vera.org. https://www.vera.org/news/the-united-states-criminalizes-people-who-need-health-care-and-housing. [Accessed 03-10-2025].

[46] Bryce Clayton Newell, M. C. K. Painting the narrative: Police body-worn cameras, report writing, and the techno-regulation of policework. *First Monday 28*, 7 (2023). https://doi.org/10.5210/fm.v28i7.13243.

[47] Buolamwini, J., and Gebru, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (23–24 Feb 2018), S. A. Friedler and C. Wilson, Eds., vol. 81 of *Proceedings of Machine Learning Research*, PMLR, pp. 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html.

[48] Cao, L. Surveillance ordinances in five u.s. cities. https://texastipi.org/surveillance-ordinances-in-five-u-s-cities/, Sep 2022.

[49] Cebreros, J. Facial Recognition Technology and Wrongful Arr ongful Arrests in the Digital ests in the Digital Policing Era. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1080&context=wlro, 2025. [Accessed 10-11-2025].

[50] Chidi, G. "creepy surveillance": Why some cities are shutting down flock cameras amid privacy concerns, Apr 2026.

[51] Citron, D. K., and Pasquale, F. The scored society: Due process for automated predictions. *Wash. L. Rev. 89* (2014), 1.

[52] COMMUNITY LEGAL AID SOCIETY, I. The state of solitary: Restrictive housing and treatment of incarcerated delawareans with mental illness. https://www.declasi.org/wp-content/uploads/2024/09/Report-The-State-of-Solitary-September-2024.pdf, 2024. [Accessed 03-10-2025].

[53] Cox, J. Cops Used Flock to Monitor No Kings Protests Around the Country — 404media.co. https://www.404media.co/cops-used-flock-to-monitor-no-kings-protests-around-the-country/, 2025. [Accessed 29-12-2025].

[54] Cox, J. ICE, Secret Service, Navy All Had Access to Flock's Nationwide Network of Cameras — 404media.co. https://www.404media.co/ice-secret-service-navy-all-had-access-to-flocks-nationwide-network-of-cameras/, 2025. [Accessed 18-12-2025].

[55] Davis, A. Y. *Are prisons obsolete?* Open Media Book. Seven Stories Press, 2011.

[56] Davis, A. Y., Alternative Radio (Boulder, Colo.), p., and Barsamian, D. The prison industrial complex, 1997 - 1997.

[57] Davis, A. Y., and Shaylor, C. Race, gender, and the prison industrial complex: California and beyond. *Meridians 2*, 1 (2001), 1–25.

[58] Davis, M. Hell factories in the field, 1995.

[59] Dixon, J. A., and Mahoney, B. The effect of accent evaluation and evidence on a suspect's perceived guilt and criminality. *The Journal of Social Psychology 144*, 1 (2004), 63–73. PMID: 14760965.

[60] Dobbins, T. Protecting the unpopular from the unreasonable: warrantless monitoring of attorney client communications in federal prisons. *Catholic University Law Review 53*, 2 (2004), 295–346.

[61] Dou, E. ICE amps up its surveillance powers, targeting immigrants and antifa. https://www.washingtonpost.com/technology/2025/10/17/ice-surveillance-immigrants-antifa/, 2025. [Accessed 18-12-2025].

[62] Duffy, C., and Williams, E. How AI is being used by police departments to help draft reports. CNN, Aug. 2025. https://www.cnn.com/2025/08/12/tech/ai-police-reports-axon.

[63] Eagly, I., and Shafer, S. Measuring "in absentia" removal in immigration court. *University of Pennsylvania law review 168*, 4 (2020), 817–876.

[64] Eubanks, V. Automating inequality : how high-tech tools profile, police, and punish the poor, 2018 - 2017.

[65] Farrar, M. Cambridge ends contract for license plate cameras after "breach of trust", Dec 2025.

[66] Fergus, R. Biased Technology: The Automated Discrimination of Facial Recognition — aclu-mn.org. https://www.aclu-mn.org/en/news/biased-technology-automated-discrimination-facial-recognition, 2024. [Accessed 10-11-2025].

[67] Ferguson, A. G. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, 1 ed. NYU Press, New York, 2017.

[68] Ferguson, A. G. Concerns about ai-written police reports spur states to regulate the emerging practice. https://policinginsight.com/feature/opinion/concerns-about-ai-written-police-reports-spur-states-to-regulate-the-emerging-practice/, 2025. [Accessed 01-24-2025].

[69] Ferguson, A. G. Generative suspicion and the risks of ai-assisted police reports. *Northwestern University Law Review 120*, 2 (2025), 299–363. https://scholarlycommons.law.northwestern.edu/nulr/vol120/iss2/9.

[70] Floberg, D., and McDermott, M. The slow death of a prison profiteer: How activism brought securus to the brink, Apr 2024.

[71] for Digital Ethics, C., and Policy. : Loyola University Chicago — luc.edu. https://www.luc.edu/digitalethics/researchinitiatives/essays/archive/2018/sentencebynumbersthescarytruthbehindriskassessmentalgorithms/, 2018. [Accessed 10-11-2025].

[72] for Human Rights, U. C. Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement. https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/, 2025. [Accessed 30-12-2025].

[73] Foucault, M. *Discipline and Punish: The birth of the prison.* Vintage Books, 1979.

[74] Gates, K. Policing as digital platform. *Surveillance & Society 17*, 1/2 (2019), 63–68. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12940.

[75] Gilmore, R. W. In the Shadow of the Shadow State — sfonline.barnard.edu. https://sfonline.barnard.edu/ruth-wilson-gilmore-in-the-shadow-of-the-shadow-state/, 2016. [Accessed 30-12-2025].

[76] Gilmore, R. W., Toscano, A., and Bhandar, B. The Prison-Industrial Complex Goes Beyond Cops and Jails. It's All Around Us. — jacobin.com. https://jacobin.com/2022/08/prison-industrial-complex-race-capitalism-abolitionism, 2022. [Accessed 30-12-2025].

[77] Glass, M. Algorithms Were Supposed to Reduce Bias in Criminal Justice—Do They? — bu.edu. https://www.bu.edu/articles/2023/do-algorithms-reduce-bias-in-criminal-justice/, 2023. [Accessed 15-04-2026].

[78] Green, B. The false promise of risk assessments: epistemic reform and the limits of fairness. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (New York, NY, USA, 2020), FAT* '20, Association for Computing Machinery, p. 594–606.

[79] Guariglia, J. K. a. M. Ring Reveals They Give Videos to Police Without User Consent or a Warrant, July 2022. https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant.

[80] Guberek, T., McDonald, A., Simioni, S., Mhaidli, A. H., Toyama, K., and Schaub, F. Keeping a low profile? technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018), CHI '18, Association for Computing Machinery, p. 1–15.

[81] Hallsby, A. Dark sousveillance, Jul 2024.

[82] Harcourt, B. E. *Against prediction: Profiling, policing, and punishing in an actuarial age.* University of Chicago Press, 2019.

[83] Hardee, C., and Torphy, M. Statement of Christopher Hardee and Micheal Torphy to the Senate Judiciary Committee, July 2025. https://www.fbi.gov/news/speeches-and-testimony/statement-of-christopher-hardee-and-micheal-torphy-to-the-senate-judiciary-committee.

[84] Harwell, D. Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns. *The Washington Post* (Aug. 2019).

[85] Hayes, Myaisha, A. D. V. How Face Recognition Fuels Racist Systems of Policing and Immigration — And Why Congress Must Act Now | ACLU, July 2021. https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now.

[86] Hoffman, J. Sousveillance (published 2006), Dec 2006.

[87] Hofmann, V., Kalluri, P. R., Jurafsky, D., and King, S. Dialect prejudice predicts ai decisions about people's character, employability, and criminality, 2024.

[88] Horowitz, J. Amazon and Microsoft stopped working with police on facial recognition. For others it's still big business | CNN Business, July 2020.

[89] HumanRightsWatch. Ill-Equipped — hrw.org. https://www.hrw.org/report/2003/10/22/ill-equipped/us-prisons-and-offenders-mental-illness. [Accessed 03-10-2025].

[90] IAPP. US State Privacy Legislation Tracker — iapp.org. https://web.archive.org/web/20260101072120/https://iapp.org/resources/article/us-state-privacy-legislation-tracker, 2025. [Accessed 01-07-2026].

[91] ICEBlock.app. Iceblock. https://www.iceblock.app/.

[92] Initiative, E. J. As Major U.S. Banks Stop Funding Private Prisons, Companies Seek Money Abroad.

[93] Initiative, P. P. American Correctional Association — prisonpolicy.org. https://www.prisonpolicy.org/aca.html, 2025. [Accessed 18-12-2025].

[94] Initiative, P. P., and Wagner, W. S. a. P. Mass Incarceration: The Whole Pie 2025.

[95] International, A. USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research, Feb. 2022. https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/.

[96] James, D. J., and Glaze, L. E. Mental Health Problems of Prison and Jail Inmates. https://static.prisonpolicy.org/scans/bjs/mhppji.pdf. [Accessed 03-10-2025].

[97] James P. McLoughlin Jr., Fielding E. Huseth, C. R. P. Challenging prosecutorial use of a pretrial detainee's electronic communications. *Southern California Review of Law and Social Justice 33*, 1 (2024), 89–130.

[98] Joffe-Block, J. Why some cities are ditching their flock license plate readers, Feb 2026.

[99] Joh, E. E. The undue influence of surveillance technology companies in policing. *NYUL Rev. Online 92* (2017), 19.

[100] Johnson, A., Egan, E., and Londoño, J. Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms — itif.org. https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/, 2023. [Accessed 15-04-2026].

[101] Johnson, Natasha N., T. L. J. Police Facial Recognition Technology Can't Tell Black People Apart. https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/.

[102] Kaba, F., Lewis, A., Glowa-Kollisch, S., Hadler, J., Lee, D., Alper, H., Selling, D., MacDonald, R., Solimo, A., Parsons, A., and Venters, H. Solitary confinement and risk of self-harm among jail inmates. *American Journal of Public Health 104*, 3 (2014), 442–447. PMID: 24521238.

[103] Kalluri, P. R., Agnew, W., Cheng, M., Owens, K., Soldaini, L., and Birhane, A. Computer-vision research powers surveillance technology. https://doi.org/10.1038/s41586-025-08972-6.

[104] Kang, J., Agudo, M., and Wonsun Hahn, J. The data behind prison reform. https://www.brennancenter.org/our-work/research-reports/data-behind-prison-reform, Sep 2025.
[105] Karakatsanis, A. The Body Camera: The Language of our Dreams. https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/f/4764/files/2024/07/Alec-Karakatsanis_The-Body-Camera-FINAL.pdf, 2024. [Accessed 10-11-2025].
[106] Kaspersen, A., and Wallach, W. Why Are We Failing at the Ethics of AI? — carnegiecouncil.org. https://www.carnegiecouncil.org/media/article/why-are-we-failing-at-the-ethics-of-ai, 2021. [Accessed 30-12-2025].
[107] Kever, J. Information Technology Can Save Police Lives, According to a New Study — uh.edu. https://www.uh.edu/news-events/stories/2019/december-2019/12112019-pavlou-police-it.php, 2019. [Accessed 15-04-2026].
[108] Kim, C. Private prisons face an uncertain future as states turn their backs on the industry, Dec. 2019.
[109] King, S., Vaughn, A., and Dunbar, C. Dialect on Trial: Raciolinguistic ideologies in perceptions of AAVE and MAE codeswitching. https://repository.upenn.edu/entities/publication/ca4e6c98-4895-4c9d-b9c1-9333cbba96b5, 2022. [Accessed 18-12-2025].
[110] Knefel, J. Meet the Private Companies Helping Cops Spy on Protesters, Oct. 2013. https://www.rollingstone.com/politics/politics-news/meet-the-private-companies-helping-cops-spy-on-protesters-117113/.
[111] Kocher, A. Glitches in the digitization of asylum: How cbp one turns migrants' smartphones into mobile borders. *Societies 13*, 6 (2023).
[112] Koebler, J. Flock Exposed Its AI-Powered Cameras to the Internet. We Tracked Ourselves — 404media.co. https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves/?ref=daily-stories-newsletter, 2025. [Accessed 29-12-2025].
[113] Koebler, J., and Cox, J. ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows — 404media.co. https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/, 2025. [Accessed 18-12-2025].
[114] Kulkarni, P., Liu, Y., Fu, H.-M., Yang, S., Gunasekara, I., Peloquin, M., Spitzer-Williams, N., Zhou, X., Liu, X., Ji, Z., and Ibrahim, Y. Auto-drafting police reports from noisy asr outputs: A trust-centered llm approach, 2025.
[115] Kurinec, C. A., and Weaver, C. A. "sounding black": Speech stereotypicality activates racial stereotypes and expectations about appearance. *Frontiers in psychology 12* (2021), 785283–.
[116] Lacy, A. Two Companies Fight to Corner the Police Body Camera Market, Dec. 2021.
[117] Lamica, J. Whether Private or Public, Prisons Profit. https://morethanourcrimes.org/voices/private-or-public-prisons-profit/.
[118] Lauron, S. The Police Shortage Crisis: How AI Can Help | Rev — rev.com. https://www.rev.com/blog/police-shortage, 2026. [Accessed 15-04-2026].
[119] Lee, N. T., Lee, N. T., and Chin-Rothmann, C. Police surveillance and facial recognition: Why data privacy is imperative for communities of color. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.
[120] LeoTech. Verus Featured in Sheriff & Deputy Magazine - LeoTech — leotechnologies.com. https://leotechnologies.com/news-resources/verus-featured-in-sheriff-deputy-magazine/, 2022. [Accessed 19-12-2025].
[121] LeoTech. Verus - LeoTech — leotechnologies.com. https://leotechnologies.com/verus/, 2025. [Accessed 19-12-2025].
[122] Lev-Ari, S., and Keysar, B. Why don't we believe non-native speakers? the influence of accent on credibility. *Journal of Experimental Social Psychology 46*, 6 (2010), 1093–1096.
[123] Libby, K. How Silicon Valley is making cops worse at their jobs, Aug. 2020. Section: All Salon.
[124] Lipton, B. Beware the Bundle: Companies Are Banking on Becoming Your Police Department's Favorite "Public Safety Technology" Vendor, May 2025.
[125] Lusoli, A., and Gilliard, C. Luxury surveillasnce: Digital democracies institute, Mar 2023.
[126] Makar, Z. The digital prison panopticon. *Harvard Journal of Law & Technology 38*, 4 (2025), 961–1026. https://jolt.law.harvard.edu/assets/articlePDFs/v38.4/1-Makar.pdf.
[127] Martin, L., and Mann, M. Locked in: Digital colonialism and the platformed prison, 2025. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/18230.
[128] Moreno-Lozano, L. Austin drops ai surveillance cameras from consideration as residents raise privacy concerns, Oct 2025.
[129] Moulton, M. Is Technology the Answer to Police Staffing Issues? — govtech.com. https://www.govtech.com/voices/is-technology-the-answer-to-police-staffing-issues, 2024. [Accessed 15-04-2026].
[130] Nadeem, M., Bethke, A., and Reddy, S. Stereoset: Measuring stereotypical bias in pretrained language models, 2020.
[131] Newell, B. C. Police visibility : privacy, surveillance, and the false promise of body-worn cameras, 2021 - 2021.
[132] Newell, B. C., Moon, N. P. Y. E., and III, H. J. P. Regulating the data market: The material scope of american consumer data privacy law. *University of Pennsylvania Journal of International Law 45*, 4 (2024), 1055–1143. https://scholarship.law.upenn.edu/jil/vol45/iss4/4/.
[133] NIST. NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software — nist.gov. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software, 2019. [Accessed 10-11-2025].
[134] of Justice, V. I. https://vera-institute.files.svdcdn.com/production/downloads/publications/alternatives-to-policing-community-violence-intervention-fact-sheet.pdf, Aug 2021.

[135] of Justice, V. I. https://vera-institute.files.svdcdn.com/production/downloads/publications/alternatives-to-policing-school-safety-fact-sheet.pdf?dm=1630432734, Aug 2021.
[136] of Justice, V. I. https://vera-institute.files.svdcdn.com/production/downloads/publications/alternatives-to-policing-traffic-enforcement-fact-sheet.pdf, Aug 2021.
[137] of Justice, V. I. https://vera-institute.files.svdcdn.com/production/downloads/publications/alternatives-to-policing-civilian-crisis-response-fact-sheet.pdf, Aug 2021.
[138] of Law, A. M. S. Can Algorithms lessen The Bias in The Criminal Justice System | Ave Maria School of Law — avemarialaw.edu. https://www.avemarialaw.edu/can-algorithms-lessen/, 2024. [Accessed 15-04-2026].
[139] of Mental Illness, N. A. Mental Health Treatment While Incarcerated — nami.org. https://www.nami.org/advocacy/policy-priorities/improving-health/mental-health-treatment-while-incarcerated/. [Accessed 03-10-2025].
[140] of WA, A. https://www.aclu-wa.org/press-releases/seattle-city-council-passes-ordinance-regulate-surveillance-technology/, Aug 2017.
[141] Office, U. G. A. Alternatives to Detention: ICE Needs to Better Assess Program Performance and Improve Contract Oversight. https://www.gao.gov/products/gao-22-104529, 2022. [Accessed 19-12-2025].
[142] Okidegbe, N. When They Hear Us: Race, Algorithms and The Practice of Criminal Law. https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4552&context=faculty_scholarship, 2020. [Accessed 10-11-2025].
[143] Okidegbe, N. Beyond More and More Accurate Algorithms: T ate Algorithms: Takeaways from McClesk om McCleskey Revisited. https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4552&context=faculty_scholarship, 2023. [Accessed 10-11-2025].
[144] on Civil Rights, U. C. U.S. Commission on Civil Rights Releases Report: The Civil Rights Implications of Cash Bail — usccr.gov. https://www.usccr.gov/news/2022/us-commission-civil-rights-releases-report-civil-rights-implications-cash-bail, 2022. [Accessed 18-12-2025].
[145] One, A. D. Axon. https://www.axon.com/in/products/draft-one, 2025. [Accessed 30-12-2025].
[146] Oregon, D. R. Solitary Confinement of Individuals with Mental Illness in Oregon's State Penitentiary Behavioral Health Unit. https://static1.squarespace.com/static/6387d767fc8a755e41aa5844/t/646d8ee1438d85376c8ad467/1684901613586/Behind-the-Eleventh-Door-Electronic-Version.pdf. [Accessed 03-10-2025].
[147] Owens, K., Alem, A., Roesner, F., and Kohno, T. Electronic monitoring smartphone apps: An analysis of risks from technical, Human-Centered, and legal perspectives. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA, Aug. 2022), USENIX Association.
[148] Owens, K., Cobb, C., and Cranor, L. "you gotta watch what you say": Surveillance of communication with incarcerated people. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021).
[149] Owens, K., Eiger, Y., Radka, B., Kohno, T., and Roesner, F. Understanding experiences with compulsory immigration surveillance in the u.s. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA, 2025), FAccT '25, Association for Computing Machinery, p. 887–899.
[150] page, W. D. H. Predictive policing algorithms are racist. They need to be dismantled. — technologyreview.com. https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/, 2020. [Accessed 10-11-2025].
[151] Park, A. L. Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing | UCLA Law Review — uclalawreview.org. https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/, 2019. [Accessed 10-11-2025].
[152] Parks, K. Out of Sight, Out of Mind: Colorado Continues to Warehouse Mentally Ill Prisoners in Solitary | ACLU — aclu.org. https://www.aclu.org/news/prisoners-rights/out-sight-out-mind-colorado-continues. [Accessed 03-10-2025].
[153] Raher, S. Data privacy in carceral settings: The digital panopticon returns to its roots. *Northwestern University Law Review Online 119* (2024), 73–104.
[154] Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., and Denton, R. Saving face: Investigating the ethical concerns of facial recognition auditing. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (New York, NY, USA, 2020), AIES '20, Association for Computing Machinery, p. 145–151.
[155] Richardson, R., Schultz, J. M., and Crawford, K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice - NYU Law Review — nyulawreview.org. https://nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/, 2019. [Accessed 10-11-2025].
[156] Richmond, R. https://www.reimaginerichmond.org/en/alternatives-to-policing-report.
[157] Rickford, J. R., and King, S. Language and linguistics on trial: Hearing rachel jeantel (and other vernacular speakers) in the courtroom and beyond. *Language 92*, 4 (2016), 948–988.
[158] Rises, W. Worth Rises — The Prison Industrial Complex: Mapping Private Sector Players. https://worthrises.org/theprisonindustry2019.
[159] Rises, W. The prison industry: How it started, how it works, how it harms. https://static1.squarespace.com/static/58e127cb1b10e31ed45b20f4/t/621682209bb0457a2d6d5cfa/1645642294912/The+Prison+Industry+How+It+Started+How+It+Works+

and+How+It+Harms+December+2020.pdf, 2020. [Accessed 18-12-2025].

[160] Robison, M., Abderhalden, F. P., and Joiner, T. E. Dehumanization and the association with nonsuicidal self-injury and suicidal ideation in an incarcerated population. *Crisis : the journal of crisis intervention and suicide prevention 45*, 4 (2024), 287–293.

[161] ROSA, J., and FLORES, N. Unsettling race and language: Toward a raciolinguistic perspective. *Language in Society 46*, 5 (2017), pp. 621–647.

[162] Russo, J., Woods, D., Vermeer, M. J. D., and Jackson, B. A. Countering the Emerging Drone Threat to Correctional Security. https://www.rand.org/pubs/research_reports/RRA108-21.html. [Accessed 23-09-2025].

[163] Samuals, J., and Hickton, D. Investigation of the PA DOC use of Solitary Confinement on Prisoners with Serious Mental Illness and/or Intellectual DIsabillities. https://static.prisonpolicy.org/scans/DOJ_Findings_Letter_Issued_by_DOJ_2_24_2014.pdf. [Accessed 03-10-2025].

[164] Schuba, T. ICE has powerful facial recognition app Illinois cops are barred from using — with little apparent oversight — chicago.suntimes.com. https://chicago.suntimes.com/the-watchdogs/2025/10/31/ice-trump-facial-recognition-clearview-police-oversight, 2025. [Accessed 18-12-2025].

[165] security, . Drone Detection Solutions | Airspace Security | AirSight — airsight.com. https://www.airsight.com/. [Accessed 23-09-2025].

[166] Securus. Investigator Pro™. https://securustechnologies.tech/investigative/investigation/investigator-pro/, 2025. [Accessed 19-12-2025].

[167] Securus. Securus Technologies Word Alert™. https://securustechnologies.tech/investigative/investigation/word-alert/, 2025. [Accessed 19-12-2025].

[168] Segal, D. Prison Vendors See Continued Signs of a Captive Market (Published 2015) — nytimes.com. https://www.nytimes.com/2015/08/30/business/prison-vendors-see-continued-signs-of-a-captive-market.html, 2015. [Accessed 02-01-2026].

[169] SHERMAN, S. A. Many cities are rethinking the police, but what are the alternatives?: Kinder institute for urban research. https://kinder.rice.edu/urbanedge/many-cities-are-rethinking-police-what-are-alternatives, Jul 2020.

[170] Simes, J. T., Western, B., and Lee, A. Mental health disparities in solitary confinement. *Criminology (Beverly Hills) 60*, 3 (2022), 538–575.

[171] Sinha, M. The automated fourth amendment. *Emory Law Journal 73*, 3 (2024), 589–656. https://scholarlycommons.law.emory.edu/elj/vol73/iss3/2/.

[172] Smith, J. Securus Settles Lawsuit Alleging Improper Recording of Privileged Prisoner Calls | Prison Legal News — prisonlegalnews.org. https://www.prisonlegalnews.org/news/2016/sep/2/securus-settles-lawsuit-alleging-improper-recording-privileged-prisoner-calls/, 2016. [Accessed 19-12-2025].

[173] Smith, J., and Lee, M. Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege — theintercept.com. https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/, 2015. [Accessed 19-12-2025].

[174] Solove, D. J. A taxonomy of privacy. *U. Pa. l. Rev. 154* (2005), 477.

[175] Spitzer-Williams, N. Axon enhances public safety and cuts report-writing time in half using Draft One, an AI-powered solution built on Microsoft Azure | Microsoft Customer Stories — microsoft.com. https://www.microsoft.com/en/customers/story/19236-axon-enterprise-azure, 2024. [Accessed 30-12-2025].

[176] staff, C., and University, W. S. Privatized prisons lead to more inmates, longer sentences, study finds.

[177] Stanley, J. Flock Can Share Driver-Surveillance Data Even When Police Departments Opt Out, And Other Flock Developments | ACLU — aclu.org. https://www.aclu.org/news/privacy-technology/flock-massachusetts-and-updates, 2025. [Accessed 30-12-2025].

[178] Stanley, J. Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance | ACLU — aclu.org. https://www.aclu.org/news/privacy-technology/flock-roundup, 2025. [Accessed 29-12-2025].

[179] Starr, S. B. Evidence-based sentencing and the scientific rationalization of discrimination. *Stan. L. Rev. 66* (2014), 803.

[180] Stokes, E. Wrongful arrest exposes racial bias in facial recognition technology — cbsnews.com. https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/, 2020. [Accessed 10-11-2025].

[181] Stoliker, B. E., Wangler, H., Abderhalden, F. P., and Jewell, L. M. Lifetime and jail-specific suicidal ideation: Prevalence and correlates in a sample of people in jail in the united states. *International Journal of Offender Therapy and Comparative Criminology 69*, 2-3 (2025), 267–285. PMID: 37098823.

[182] Swarns, C. When Artificial Intelligence Gets It Wrong - Innocence Project — innocenceproject.org. https://innocenceproject.org/news/when-artificial-intelligence-gets-it-wrong/, 2023. [Accessed 10-11-2025].

[183] the ACA Conference, S. American Correctional Association Trade Show: Fact Sheet on Some of The Companies Involved — web.archive.org. https://web.archive.org/web/20011103204340/http://www.prisonsucks.com/ACA/ACAfactsheet.html, 2001. [Accessed 18-12-2025].

[184] the Public Interest, I. BUYING ACCESS: How Corporations Influence Decision Makers at Corrections Conferences, Trainings, and Meetings. https://www.inthepublicinterest.org/wp-content/uploads/Buying-Access-In-the-Public-Interest-PDF.pdf. [Accessed 18-12-2025].

[185] Tibbs, D. F., and Chauncey, S. From slavery to hip-hop: punishing black speech and what's "unconstitutional" about prosecuting young black men through art. *Washington University journal of law and policy 52*, 1 (2016), 33–.
[186] UK, B. BLAM UKs Statement against the Criminalisation of Black Languages. https://blamuk.org/2024/07/31/blam-uks-statement-against-the-criminalisation-of-black-languages/, 2024. [Accessed 18-12-2025].
[187] US DoJ, B. https://www.bop.gov/inmates/fsa/docs/evidence_based_recidivism_reduction_programs.pdf.
[188] Valentin, L. The first step to stop corporations from profiting from incarceration in the United States | Transnational Institute, Sept. 2025.
[189] Vande Velde, A., and Roberts, W. Rethinking boston's public safety system. http://hnmcp.law.harvard.edu/wp-content/uploads/2021/04/Rethinking-Bostons-Public-Safety-System.pdf, Dec 2020.
[190] Vant4ge. Can Corrections Trust AI with High-Profile Assessments? | AIDA by Vant4ge — helloaida.io. https://helloaida.io/can-corrections-trust-ai-with-high-profile-assessments/. [Accessed 03-10-2025].
[191] Vant4ge. Elevating the Human in the Loop with AI-Powered Collaboration | AIDA by Vant4ge — helloaida.io. https://helloaida.io/elevating-the-human-in-the-loop-with-ai-powered-collaboration/. [Accessed 03-10-2025].
[192] Vant4ge. Inmates Talk, Aida Listens: The Unexpected Benefits of AI-Driven Interviews in Corrections | AIDA by Vant4ge — helloaida.io. https://helloaida.io/inmates-talk-aida-listens-the-unexpected-benefits-of-ai-driven-interviews-in-corrections/. [Accessed 03-10-2025].
[193] Vant4ge. Hello aida. https://helloaida.io/, 2025. [Accessed 30-12-2025].
[194] Victoria Burton-Harris, P. M. Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart | ACLU — aclu.org. https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart, 2020. [Accessed 10-11-2025].
[195] Watch, H. R. Callous and Cruel — hrw.org. https://www.hrw.org/report/2015/05/12/callous-and-cruel/use-force-against-inmates-mental-disabilities-us-jails-and. [Accessed 03-10-2025].
[196] Watford, T. Unlocking the Truth: A Closer Look at Cash Bail Data — bailproject.org. https://bailproject.org/data/unlocking-the-truth/, 2023. [Accessed 18-12-2025].
[197] Weisburd, K. Punitive surveillance. *GWU Legal Studies No. 2021-37*, 6 (2022).
[198] Wendy Sawyer, P. P. I. New government report points to continuing mental health crisis in prisons and jails — prisonpolicy.org. https://www.prisonpolicy.org/blog/2017/06/22/mental_health/. [Accessed 03-10-2025].
[199] Wetzel, H. Research finds prison education programs reduce recidivism. https://www.mackinac.org/pressroom/2023/research-finds-prison-education-programs-reduce-recidivism, journal=Mackinac Center, Jan 2023.
[200] Whittaker, Z. Lawmakers say stolen police logins are exposing Flock surveillance cameras to hackers | TechCrunch — techcrunch.com. https://techcrunch.com/2025/11/03/lawmakers-say-stolen-police-logins-are-exposing-flock-surveillance-cameras-to-hackers/, 2025. [Accessed 30-12-2025].
[201] Wilkins, J. Cities are shredding their ai surveillance contracts en masse, Feb 2026.
[202] Wilson, D. Platform policing and the real-time cop. *Surveillance & Society 17*, 1/2 (2019), 69–75. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12958.
[203] with Trystan Edwards, S. K., and Belmont, J. Language Bias on Trial — Demystifying Language Project — demystifyinglanguage.fordham.edu. https://demystifyinglanguage.fordham.edu/articles/language-bias-on-trial/, 2025. [Accessed 18-12-2025].
[204] Yong, E. A Popular Algorithm Is No Better at Predicting Crimes Than Random People — theatlantic.com. https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/, 2018. [Accessed 10-11-2025].
[205] Zhong, S., Senior, M., Yu, R., Perry, A., Hawton, K., Shaw, J., and Fazel, S. Risk factors for suicide in prisons: a systematic review and meta-analysis. *The Lancet. Public health 6*, 3 (2021), e164–e174.
[206] Zuboff, S. *The age of surveillance capitalism : the fight for a human future at the new frontier of power*, first edition. ed. PublicAffairs, New York, NY, 2019 - 2019.

Generative AI Usage Statement

No AI was used for any part of the process.