

# **Hooverism as a Framework for Understanding the Historical and Unethical Nature of the Use of Artificial Intelligence and Other Surveillance Practices in the United States**

**Patricia HALEY**

*Doctoral Candidate, Capitol Technology University, Laurel, Maryland, USA*

*ORCID: <https://orcid.org/0009-0006-0188-1796>*

*patriciaaemail@gmail.com*

**Abstract:** This theoretical paper establishes Hooverism as a framework for analyzing the ideological continuities between J. Edgar Hoover's 48 year tenure as FBI director (1924-1972) and contemporary algorithmic surveillance systems. Hooverism is defined by four interconnected pillars of informational supremacy, loyalty enforcement, racialized control, and bureaucratic secrecy that structured mid-20th century domestic intelligence and now shape modern AI governance. Drawing on surveillance studies, critical data theory, and institutional history, I demonstrate that contemporary biometric surveillance, predictive policing, and algorithmic risk assessment automate and scale Hooverist logic rather than transcending it. Through systematic analysis of historical precedents and modern developments in algorithmic governance, I trace how informational supremacy manifests as mass data collection justified by security claims; loyalty enforcement operates through automated flagging of "suspicious" behavior without criminal predicates; racialized control persists through biased training data and discriminatory deployment; and bureaucratic secrecy functions through vendor nondisclosure agreements (NDA) and algorithmic opacity. This pattern reveals that surveillance ideology precedes and transcends specific technologies. AI amplifies existing institutional practices rather than creating new forms of bias. The framework demonstrates that legislative reforms addressing individual technologies prove inadequate because they fail to disrupt underlying ideological structures. I provide the Hooverism framework, which establishes six governance principles: equity, ethics, transparency, stakeholder engagement, oversight, and democratic accountability, with operational protocols for bias auditing, community consent mechanisms, and sunset provisions. This framework enables policymakers and scholars to identify when algorithmic systems automate historical injustice rather than technical error, supporting interventions that address root causes rather than symptoms. By exposing how surveillance becomes normalized through the language of security and administrative neutrality, this analysis provides conceptual tools for resisting governance through suspicion and establishing democratic accountability in the era of algorithmic governance.

**Keywords:** Biometric surveillance, algorithmic governance, AI surveillance, Hooverism (Hoover Era Policing), Ethics, Accountability, Human Rights, Predictive Policing

## Introduction

This inquiry presents *Hooverism* as a conceptual framework based on the political and institutional practices (Cecil, 2014; Chalmers, 1992) established during J. Edgar Hoover's 48 year tenure leading the Federal Bureau of Investigation (Cecil, 2014). It represents an attempt to understand the ongoing transformation of surveillance ideology in contemporary America. The deployment of algorithmic surveillance is sufficiently high to warrant an urgent examination and audit of the ideological principles underlying the digital systems used in policing. Today, over 85% of federal agencies utilize various algorithmic technologies, incorporating automated surveillance into their daily governance and law enforcement practices (Haley, 2025b; U.S. Government Accountability Office [GAO], 2023). Hooverism was not only about surveillance, but also about governing through suspicion, referring to the period when the foundational principles of democracy and the democratic code began to diverge. This core code serves as the theoretical construct that reflects the operationalization of bias and institutional priorities of Hoover.

Hooverism exemplifies the shift toward using surveillance instead of governing constraints, driven by fear based ideology. Although governance and the practical application of surveillance technologies are designed to improve public safety, there is limited evidence to confirm a direct link to reduced violence (Haley, 2025b). Therefore, it is essential to explore additional positive uses for civil society while maintaining strict accountability to ensure accuracy and transparency. This article argues that no one should be excluded from society's demands for data, limits on personal data as a commodity, and clear sharing outcomes and restrictions. It promotes education to encourage community involvement, regular data audits, transparency, and ethical standards in programming. Formal alternatives to legislative reforms, such as efforts focused on algorithmic transparency, increased public oversight, and ethical design of surveillance systems are inadequate and lag technological advancements. Hooverism presents a framework for integrating algorithmic tools used in policing in a fair, practical, and responsible way. This approach fosters understanding and accountable governance in a changing world, preventing the unchecked expansion of an authoritarian digital landscape (Cecil, 2014; Haley & Burrell, 2025b).

Hooverism's four intertwined pillars informational supremacy, loyalty enforcement, racialized control, and bureaucratic secrecy are rooted in mid20th century American domestic intelligence. It established a governance model based on suspicion, often targeting marginalized communities and political dissidents (Theoharis, 2004). Modern surveillance tools such as predictive policing, immigration risk scoring, and facial recognition are technological evolutions of this legacy, automating long standing patterns of political and racial control under the pretense of efficiency and public safety (Brayne, 2020; Eubanks, 2018; Zuboff, 2019). Academic research has examined the technical advancements of policing tools and the social impacts of algorithmic technology; this paper explicitly links scholarly and practical insights to the ideological roots of Hoover's institutional framework and current surveillance practices. By situating these modern systems within an academic context, the analysis can better explore the underlying influences shaped by Hooverism's ideological spectrum. This article emphasizes the systemic issues caused by the persistent accumulation of mission creep, racial bias, and bureaucratic opacity, which continue to weaken democratic governance (Benjamin, 2019; Couldry & Mejias, 2019). In doing so, it calls for a normative critique of how surveillance is normalized, legitimized, and given cumulative power through the language of national security and administrative neutrality (Monahan, 2006).

This article's primary contribution is the introduction of Hooverism as an articulation that it is not technology alone, but ideology that transforms life, both academically and

practically. Hooverism may be understood as a conceptual soliloquy in which the intertwined nature of intelligence, law enforcement, institutional control, and public perception is understood as an uninterrupted projection of historical authority. It provides researchers with a historical anchor in debates over security, privacy, and democratic accountability to explore the decisive role of surveillance empirically and to inform policy discussions about large language models, artificial general intelligence, algorithmic transparency, and human rights protections. Hooverism's intertwined pillars provide a foundational precedent through which to examine the core code, going beyond source code, algorithmic models, training data, embedded biases, machine learning, and institutional assumptions that shape their functions and outcomes. This core code increasingly integrates with or replaces traditional intelligence, law enforcement, and governance methods, which are vitally important for protecting democratic values (Haley & Burrell, 2025c; Harcourt, 2015; Zuboff, 2019).

Surveillance is not a new phenomenon; institutions have long gathered intelligence to maintain order and power. However, Hooverism embodies an ideological framework that, combined with political loyalty, racial targeting, informational dominance, and bureaucratic secrecy, has evolved into a more sophisticated system driven by algorithms that operate beyond human control. These systems position everyone as both watcher and watched, blurring traditional boundaries and making surveillance more pervasive, impersonal, and easily employed through modern technology, presenting new challenges to regulation. This article proposes Hooverism not as a historical anecdote, but as an enduring conceptual lens for bias mitigation, efficient model training, and accuracy in outcomes crucial in the rapid advancements in artificial intelligence (AI) and emphasis on the importance of regulatory frameworks to prevent loss of control or an autonomous relevant surveillance state (Ferguson, 2017; Haley, 2025a).

## Problem Statement

The rise of biometric surveillance in the United States reflects more than just technological progress; it also embodies a persistent ideology rooted in suspicion, racialized control, and bureaucratic secrecy, what this paper calls *Hooverism*. Originating from the institutional legacy of J. Edgar Hoover's 48 year tenure as FBI Director, Hooverism illustrates how surveillance systems have historically worked to normalize government overreach and enforce loyalty through opaque, data driven methods (Cecil, 2014; Theoharis, 2004). Today, modern surveillance tools, such as facial recognition, predictive policing, and algorithmic risk assessment, continue this trend not as neutral efficiency tools but as political devices influenced by long standing ideologies (Eubanks, 2018; Haley, 2025b; Zuboff, 2019). This issue is urgent, as over 85% of federal agencies already use algorithmic technologies that reinforce bias and weaken democratic accountability (GAO, 2023; Haley, 2025b). If left unchecked, this ideological tradition risks solidifying governance based on fear and masking systemic inequality under the pretense of security. A comprehensive framework is therefore needed to recognize, critique, and challenge the persistence of Hooverist logic in the digital age, along with addressing related ethical concerns.

## Purpose Statement

The purpose of this conceptual paper is to introduce *Hooverism* as a theoretical framework that reveals the ideological continuities between mid20thcentury intelligence practices and modern algorithmic surveillance systems. By combining insights from critical data theory, surveillance studies, and institutional history, the paper presents Hooverism as a collection of ideas centered on informational dominance, loyalty enforcement, racialized control, and bureaucratic secrecy that support contemporary surveillance structures (Benjamin, 2019; Brayne, 2020; Haley & Burrell, 2025c). This paper establishes Hooverism as a theoretical

framework that demonstrates how surveillance ideology, embedded during Hoover's FBI directorship structures contemporary algorithmic governance. I provide conceptual tools for identifying when bias reflects the reproduction of systematic ideology rather than technical failure, enabling interventions that address root causes rather than symptoms. This aligns with broader calls for ethical transparency in algorithms, protection of human rights, and democratic accountability in managing AI and data infrastructures (Ferguson, 2017; Zuboff, 2019).

### **Significance Statement**

This inquiry is important because it reframes biometric and algorithmic surveillance not just as issues of privacy or technological progress, but also as expressions of a deeply rooted ideological framework that threatens democratic principles and ethics. By using *Hooverism* as a conceptual lens, the paper provides a historically grounded and theoretically rich vocabulary for understanding how surveillance becomes normalized, justified, and continued within democratic institutions (Cecil, 2014; Harcourt, 2015). The analysis creates a necessary link between historical patterns of state control and current discussions on data ethics, algorithmic accountability, and public oversight. As legislative responses remain slow and inadequate, especially with the rapid development of AI technologies, it becomes crucial to develop critical frameworks for democratic resistance (Couldry & Mejias, 2019; Haley, 2025b). The paper's originality lies in how it repositions Hooverism not as an archival relic, but as a living model that influences digital governance, helping to shape academic, policy and civic reactions to a technology driven surveillance state in which ethics often take a backseat to innovation.

### **Nature of the Inquiry**

This theoretical inquiry examines surveillance ideology through an interpretive analysis that links historical intelligence strategies with contemporary algorithmic systems. Rather than testing hypotheses through controlled experiments, I demonstrate pattern continuity across contexts, providing explanatory frameworks validated through their capacity to account for otherwise disparate phenomena. This methodology establishes theoretical frameworks through systematic analysis, following established traditions in critical theory, surveillance studies, and institutional analysis (Haley & Burrell, 2025b; Monahan, 2006). Through this perspective, the paper examines how core Hooverist logics are revived in today's digital infrastructures, often under the pretense of neutrality, efficiency, or public safety (Benjamin, 2019; Eubanks, 2018). Consequently, this inquiry provides both a diagnostic and normative contribution: it clarifies how surveillance functions ideologically and demonstrates new ethical and political frameworks for resisting governance by fear in the age of algorithms.

### **Literature Review**

#### ***Historical Roots of Surveillance Governance***

J. Edgar Hoover, born in 1895 in Washington, DC, joined the Justice Department in 1917 and became Director of the Bureau of Investigation in 1924, a position he held until his death in 1972 (Chalmers, 1992). In 1935, the Bureau of Investigation was renamed the Federal Bureau of Investigation. As Cecil (2014) pointed out, Hoover ignored orders to end the loyalty investigations during the Red Scare era and continued to maintain secret lists and centralized records. This practice set the stage for a bureaucratic culture characterized by unchecked surveillance power, claiming to protect both the public and individual civil liberties. In 1919 and 1920, J. Edgar Hoover, under the direction of Attorney General A. Mitchell Palmer, led the Palmer Raids, which marked the early foundations of Hooverism

raids driven by suspicion rather than evidence. During these raids, approximately 10,000 individuals, mainly anarchists and communists, were arrested despite limited evidence; two thirds of those arrested were released shortly afterward, while around 3,500 were detained for deportation proceedings. As Cecil argued, these events show that Hooverism operated not just as a surveillance tool, but also as a broader system of governance rooted in preemptive criminalization. The bureau was never held accountable, even after efforts by the ACLU to expose its unlawful practices, including burglary, wiretapping, and political surveillance in a pamphlet titled “The Nationwide Spy System Centering on the Department of Justice,” which depicted the FBI as a secret political police force. Hoover dismissed the claims and suggested that the pamphlet leaned toward communist sympathies. Over the years, multiple attempts have been made to remove these abuses from the Bureau’s record and to address Hoover’s personal history.

In 1940, the Hatch Act imposed restrictions on federal employees from affiliating with organizations deemed subversive, a broad interpretation that Hoover relied on. Hoover used this authority not only to target political dissenters, but also to scrutinize journalists through a sophisticated public relations campaign aimed at shaping public perception of the FBI and isolating critics. Generally, journalists’ credibility was judged by their perceived influence and ability to mold public opinion. This is documented in the FBI’s *Molders of Public Opinion* report, which negatively portrayed dissenting critics as unAmerican and potentially linked to subversive activities, or sometimes even targeted journalists for arrest under the constitutional detention index. The report reflects decades of passive monitoring and active investigations targeting hundreds of American journalists, with the goal of discrediting, disrupting, or silencing dissent. Through these efforts, Hoover managed narrative control and created legitimacy by covertly surveilling to suppress criticism and maintain the image of a lawful federal agency (Cecil, 2014). This reinforces two key pillars of Hooverism loyalty enforcement and informational dominance by illustrating how media manipulation and suppression served as practical tools of ideological control.

The rise of COINTELPRO (CounterIntelligence Program) established covert action strategies aimed at domestic political groups and individuals in the United States. These operations were designed to disrupt and neutralize civil rights leaders, labor organizers, environmentalists, feminists, members of the American Indian Movement, animal rights advocates, antiwar protesters, and leftwing organizations. Hoover engaged in anonymous smear campaigns, forged letters, fabricated threats, and engaged in efforts to incite internal conflicts. These techniques are derived from wartime counterintelligence practices (Church Committee, 2020; Theoharis, 2004), reflecting the core principles of Hooverism: information dominance, controlled biases, loyalty enforcement, and bureaucratic secrecy. COINTELPRO demonstrates how Hoover operationalized an ideology rooted in control and suspicion, showing how domestic surveillance was used not to promote democratic principles but to suppress dissent, thereby embedding authoritarian principles deeply within U.S. intelligence practices.

Hooverism highlights that the intertwined pillars serve as an analogy for the algorithmic code and what should symbolize the democratic code. The use of surveillance changed with Hoover. His nearly half century tenure, from 1924 to 1972, led the FBI to expand its role and powers in law enforcement and intelligence, establish a centralized fingerprint database, adopt investigative procedures and standards, and broaden its intelligence collection capabilities. Theoharis (2004) explained that he adopted suspicion based intelligence as a core strategy, rather than a legal exception. Buolamwini (2023) and Noble (2018) explored the ideological foundation of modern algorithmic systems that are embedded with search algorithms and architecture under the surface of objectivity. Methods like predictive policing and biometric monitoring repeat Hooverism’s focus on control instead of accountability, showing how current technologies inherit, rather than surpass,

past abuses without seeking protections within the human rights framework. This undermines the normative definition of the right to privacy. Recognizing this continuity is crucial for any meaningful reform (Haley & Burrell, 2025b; Teo, 2025).

### **Surveillance Ideology and Governmentality**

Foucault (1995) argued that modern institutions rely on surveillance mechanisms to make individuals visible and manageable, allowing authorities to categorize, profile, and oversee populations under the watch of power. Foucauldian logic provides a critical perspective for understanding how state authorities regulate populations through surveillance, normalization, and subtle power exercises, extending beyond mere coercion to continuous data collection. In this framework, algorithmic policing automates control mechanisms based on predictive risk and automated suspicion at a digital scale. Analyzing widespread biometric surveillance systems reveals an increase in involuntary public monitoring through various AI technologies such as facial recognition, fingerprint analysis, iris scanning, gunshot detection, and surveillance cameras, all claiming to enhance public safety (Haley, 2025a). Zuboff (2019) expanded on this analysis by introducing the concept of surveillance capitalism, which describes how capturing and commodifying digital data creates new forms of social domination. This ongoing monitoring and data collection shapes lawful behavior and public conduct while ostensibly improving security, raising serious concerns about unlimited discretion, civil liberties, and democratic accountability. This aligns with Foucault's warning about the normalization effects of disciplinary power, which molds citizen behavior through self regulation in response to constant observation (Foucault, 1991; Haley, 2025b).

Hoover's tactics involved careful strategies, including preemptive and often illegal surveillance methods that primarily targeted political dissidents, immigrants, racial minorities, and civil rights activists (O'Reilly, 1989). As Cecil (2014) noted, Hoover's tactics also included targeting, monitoring, and manipulating journalists. Hoover recognized the power of the media and used it to build the mythos of the FBI and the GMan ideal, while strategically leaking both factual and fabricated information in exchange for favorable media coverage. Hoover maintained a friends list, rewarding those who portrayed the FBI positively with exclusive access or insider stories, while journalists perceived as enemies could be targeted with anonymous threats, character assassination, and smear campaigns, like the tactics used against politicians and activists (Theoharis, 2004). Hoover's calculated strategy of intimidation, blacklisting, and leaks, along with active suppression of dissenting media voices, helped to sustain a perception of mistrust, partly because the public uncritically trusted journalism and a dominant cultural narrative that framed agencies like the FBI as inherently benevolent and patriotic (Cecil, 2014; O'Reilly, 1989). This merging of surveillance and public trust normalized suspicion as a form of governance. Instead of following legal transparency, the FBI under Hoover operated through discretionary authority, creating systems that demanded loyalty and suppressed dissent. Hooverism, as defined here, is not just a legacy of one individual, but also a broader ideological stance in which surveillance becomes a governing tool marked by informational dominance, racialized control, and bureaucratic secrecy (Harcourt, 2015; Monahan, 2006).

### **The Illusion of Neutral and The Language of Legitimacy**

Data neutrality is just an illusion controlled and shaped by secrecy and power feedback loops (Borat, 2025). In 2016, the RAND Corporation documented this systematic error by forecasting the accuracy of a Chicago police predictive strategic suspect list (SSL) or most wanted list of individuals likely to be arrested. The results showed that out of 426 named at risk individuals, there was no difference between their likelihood of committing homicides and of becoming victims of homicides, and they were more likely to be arrested for

shootings. Chicago found no change in the city's homicide rates. Later that same year, Chicago police reported an improvement in its heat list accuracy, claiming 80% SSL accuracy in arrests involving shootings, with more than 70% of those shot in Chicago being on the SSL. Pointedly, there seems to be improvement; however, the list still functions as a police target list rather than an intervention map to stop violence (Ferguson, 2017). This pattern of technologically mediated suspicion echoes Hoover era intelligence practices, in which the FBI's authority was masked as neutral expertise. In both cases, objectivity is strategically claimed while information acts as a tool of dominance whether through Hoover's files or modern invisible algorithms operating in a vacuum to shape perceived public perception. These systems focus not on actual risk, but on precriminality and risk profiling, reinforcing suspicion through interpretive frameworks that hide accountability (Borat, 2025; Ferguson, 2017; Neyland, 2006).

Hooverism normalized surveillance by framing it in bureaucratic language of neutrality. Big data policing is no longer a futuristic concept but a complex black box of data, with over 4,000 databases collecting information on everyone (Ferguson, 2017). Terms like *national security*, *illegal immigrant*, *driver*, and *data subject* reduce people to simple abstractions (Monahan, 2006). This linguistic framing, carried into algorithmic systems, turns the targeted individuals into data to be sorted and monitored rather than citizens to be engaged. Haley (2025b) and Kassler and Bowman (2023) emphasized the crucial role of language and public perception in shaping acceptance of surveillance, demonstrating how terminology used can influence public attitudes and ethical concerns related to biometric and AI technologies or commerce. This indicates that wording can either lessen or heighten fears over privacy breaches and government overreach, affecting public understanding and trust in surveillance practices. This idea connects with worries about algorithmic governance and biometric surveillance, which have roots in abuses like Hooverism, and how societal fears can significantly influence policy, acceptance, and ethical debates. It illustrates how surveillance, used by law enforcement, becomes invisible and morally unassailable through the guise of safety (Zuboff, 2019). While Hooverism relied on secrecy and public perception to build profiles, Hooverism combined with surveillance capitalism transformed this into an ideological framework in which individuals are reduced to data points, commodified, and exploited for institutional control or economic gain by capturing behavioral data for predictive and manipulative purposes.

Haley and Burrell (2025c) and Kassler (2023) advocated recognizing that these societal concerns can carry significant power and promote more nuanced communication and policy implementation with consent and transparency, rather than mitigating vague or threatening portrayals of surveillance activities, which law enforcement often conceal under sensitive pretenses. This practice can create a divide between technological progress and public trust. By integrating Haley and Burrell's and Kassler's communication centered perspective on algorithmic bias and racialized surveillance (Buolamwini, 2023; Lewis, 2021; Noble, 2018), along with an understanding of surveillance capitalism (Zuboff, 2019), we can start to demystify the ethical and policy frameworks surrounding digital surveillance. This approach not only challenges, but could also diminish Hooverist tendencies and bolster democratic legitimacy and institutional effectiveness, blurring the line between public policing and private data collection.

### **From Filing Cabinets to Algorithms**

In 1972, Justice William Rehnquist of the U.S. Supreme Court reaffirmed a fundamental democratic principle: individuals have a right to public anonymity, which can only be overridden when their actions or speech genuinely attract government interest, often due to criminal activity, an accident, or a noncriminal emergency. Peter Weston highlighted that people frequently act in public under the assumption of practical anonymity, where they

expect to be observed but not identified (Slobogin, 2007). McKay (2020) argued that the tensions among suspicion, effectiveness, secrecy, and democratic legitimacy shape the formal boundaries of modern surveillance practices, incorporating Hoover's four pillars informational supremacy, loyalty enforcement, racialized control, and bureaucratic secrecy supporting a governance structure driven by suspicion rather than accountability.

Surveillance has been extensively studied across multiple interdisciplinary fields, including surveillance studies, critical data theory, and political sociology. However, few frameworks systematically explore the historical roots of surveillance ideology and how these dynamics continue to persist and evolve within modern digital governance (GAO, 2024; Slobogin, 2007). This indicates that Hooverism as an ideological framework remains enduring because it is both historically grounded and forward looking, scaled into digital tools such as predictive policing, AI driven immigration risk assessments, and facial recognition systems. Slobogin (2007) argued that CCTV surveillance has offered no evidence that widespread CCTV programs increase public safety, provide a less costly alternative to policing, or reduce crime rates. Teo (2024) emphasized how the emotional and psychological toll of surveillance constitutes a form of slow violence, a cumulative harm to human rights often overlooked in policy discussions. Hooverism uniquely encapsulates this violence by connecting bureaucratic secrecy, racialized superstition, information dominance, and ideological control into a durable system of governance. Unlike narrower critiques, the Hooverism framework shows how surveillance functions not merely as a technical issue, but also as a historically rooted system of harm that gradually undermines civil liberties, trust, and democratic processes. This literature review synthesizes key scholarly contributions and paves the way for new interdisciplinary research, highlighting Hooverism as a distinctive ideological formation that influences ethical debates on surveillance governance.

### **The Digital Mutation**

Contemporary systems of predictive policing, immigration risk scoring, and facial recognition embody Hooverism's legacy (Brayne, 2020). What once required field agents now happens through automated databases and AI. Hooverism's core logic watch first, ask questions never remains intact, but technologically scaled. The hammer of suspicion has become a networked, automated scalpel without oversight (Eubanks, 2018).

A modern form of Hooverism appears in biocybersecurity, in which surveillance and control are no longer tied to state actors or files but are automated through digital infrastructure with minimal oversight. AI now acts as a digital scalpel, able to infiltrate genomic databases and extract sensitive biomedical data (Bloomfield et al., 2024; De Haro, 2024; O'Brien & Nelson, 2020). As Haley and Burrell (2025c) explained, this automation represents a change in power, a rise in algorithmic Hooverism. The original Hoover framework introduced four interconnected pillars: information dominance, loyalty enforcement, racialized control, and bureaucratic secrecy. It has now evolved into a digital form, allowing both private and state actors to predict, monitor, and manipulate behavior invisibly. The biological body becomes a new method of classification and preemption, determined not by law but by governed predictive AI systems trained on biased or incomplete data. To counter this shift of Hooverism, democratic societies must create regulatory frameworks that recognize AI as a form of governance, not just a tool subject to constitutional limits, transparency, and collective oversight. Without these measures, AI will continue to operate as a precise yet unaccountable scalpel and become embedded in the fabric of control.

When weaponized by malicious insiders, biometric surveillance systems can act as silent enablers of unauthorized access. In one plausible scenario, facial recognition systems, initially designed as safeguards, are manipulated to ignore threats, making physical access

control systems blind to insider breaches. These behavioral monitoring tools become instruments of deception, with their surveillance logic inverted through subtle algorithmic changes (Bloomfield et al., 2024; De Haro, 2024; O'Brien & Nelson, 2020). AI, empowered by insider threats, can identify, extract, and erase traces of critical biomedical data theft, such as proprietary vaccine research or genetic engineering blueprints, facilitating the illegal trade of biological materials. This bio crime occurs through encrypted dark web marketplaces, where AI hides transaction trails and logistics, shielding the illegal biological trade from detection. Such developments not only threaten biological security, but also reflect the ongoing ideological persistence of Hooverism. As defined in Haley and Burrell (2025a), Hooverism describes a governing approach in which surveillance infrastructure, once presumed neutral or protective, is redirected toward control, preemption, and opacity, automating suspicion and making enforcement invisible. These reoriented coercive or clandestine patterns need to be reexamined, analyzed, and redesigned to understand their broader impact on governance and global health infrastructures, prompting an active ethical reevaluation.

### From Judgement to Calculation

Joseph Weizenbaum's ethical critique of delegating judgment to machines, initially articulated in 1976, goes beyond theoretical discussion and is embedded in modern digital surveillance systems, helping to explain how Hooverism's worldview has evolved into the algorithmic era. In *Computer Power and Human Reason*, Weizenbaum (1976) warned against confusing authoritative mechanical decision making with human moral judgment, emphasizing that entrusting ethical responsibilities to machines undermines accountability and incorporates a belief system into apparently neutral, objective systems. This ongoing tension highlights the persistent conflict in surveillance governance between human moral agency and algorithmic calculation, a struggle that has lasted nearly 50 years and is especially evident today in practices like predictive policing, AI risk scoring, and immigration enforcement. By tracing this history, like Hooveristic logic, we see how the ideological and ethical issues Weizenbaum raised remain relevant from analog systems to algorithms, through monitoring practices based on suspicion and opaque decision processes, thus recreating a surveillance regime rooted in fear and ideological control. Weizenbaum's concerns about machine based judgment replacing human decision making are not just theoretical; they are structurally embedded in contemporary digital surveillance technologies, embodying a lasting tension in surveillance governance between suspicion and control.

### Hooverism and Algorithmic Governance

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 expanded surveillance capabilities related to terrorism offenses, according to U.S. Congress 18 U.S.C 2517, enhancing law enforcement's ability to detect, investigate, and prevent potential terrorist threats by increasing access to records and improving interagency information sharing. This post 9/11 legislation and the militarization of immigration enforcement extended Hooverist principles across new bureaucracies and jurisdictions (Haley, 2025b; Harcourt, 2015). Tools originally designed for foreign threats were turned inward. Active duty military tools like drones are now used at domestic borders. Hooverism persists through mission creep: the justification of expanded surveillance as a matter of efficiency and protection.

Unlike military institutions, which uphold constitutional subordination through mission command principles, domestic law enforcement has learned to operate beyond constitutional boundaries while claiming democratic legitimacy (GAO, 2023). Hooverism's four interconnected pillars show how surveillance code shifted from mission creep to

algorithmic automation: (a) information security, where the shift from investigating specific crimes to broad population monitoring evolved from Hoover's filing systems into AI data driven predictive policing technology that treats mass surveillance as an operational necessity rather than a constitutional exception; (b) loyalty enforcement, expanding from criminal investigation to political monitoring, transforming from COINTELPRO operations into algorithmic systems that automatically flag allegedly suspicious behaviors without a criminal predicate, thus monitoring populations instead of investigating crimes; (c) racialized control, normalizing targeting communities based on demographic traits instead of individual criminal behavior, migrating from systematic FBI practices into biased algorithms that encode discriminatory enforcement as data driven policing; and (d) facial recognition technology deployed under conditions of bureaucratic secrecy and algorithmic opacity, without constitutional review and oversight, rooted in operational compartmentalization.

A comparative analysis of civilian and defense research and development (R&D) shows that innovations depend on shared knowledge of context, syntax, and accuracy. This results in transparent algorithmic code and clarifies any ambiguous norms affecting people, which can falsely involve civilians as combatants or mistake infrastructure for military bases. Understanding AI logic is essential; for example, terms like *swarm* and *ant colony*, which mimic natural phenomena, are used in UAV development (Schmid et al., 2022). Ethically aligned systems are now very important because routinely applied patents and dual use technologies can spread from national security, feeding civilian surveillance systems, reinforcing Hooverist ideals, maintaining bureaucratic opacity, and solidifying entrenched power relationships (Acosta et al., 2017).

This institutional logic, transmitted through organizational culture and socialization, can lead law enforcement to view constitutional limits as obstacles rather than democratic essentials. Officers, trained within institutions that normalize constitutional violations as acceptable practices, carry out surveillance and may respond in various ways, including controversially, as a heavily militarized force to protests, using excessive force or perceiving the population as outsiders, not out of malice but because they see procedural justice as merely bureaucratic and influenced by social and political factors (Triola & Chanin, 2022). Addressing AI surveillance involves restoring mission discipline and upholding constitutional limits, like military constraints. The crisis originates from institutional cultures that, even before algorithms, operated outside constitutional boundaries, often justifying overreach as necessary. Law enforcement must function within constitutional boundaries, under civilian oversight, with clear distinctions between criminal investigation and population surveillance. Military principles also help to safeguard democracy.

## Outcomes and Resistance to Hooverist AI Governance

Hooverism, situated within a broader genealogy of American surveillance, reveals how racialized control and enforcement of political loyalty became foundational to national security practices that are foundations that continue to shape today's algorithmic systems (Benjamin, 2019; Couldry & Mejias, 2019). Hoover carefully crafted the FBI's image as a neutral and efficient agency, but public critics emerged as early as 1950. Journalist Fred J. Cook's 1958 exposé warned the public against the unchecked power of the bureau and its growing threat to civil liberties. Similarly, industrialist Cyrus Eaton condemned the FBI, citing its use of propaganda and political policing to gain power and authority. Instead of addressing these concerns, high ranking officials like Assistant Director William Sullivan portrayed such critiques as threats to national security. These early acts of resistance demonstrate that the risks of unchecked surveillance were never hidden, with critics recognizing the entrenched police power and the merging of dissent with disloyalty. This

logic persists in algorithmic systems that label individuals as high risk based on opaque data and inherited biases. Such algorithmic risks Joh (2018) explained, involves assigning risk scores that can influence law enforcement to increase surveillance, conduct home visits, or make arrests, often leading to errors and biases that result in wrongful stops, wrongful arrests, and unjustified use of force. The digital evolution of Hooverism is evident in predictive policing algorithms, immigration risk scoring systems, and facial recognition technologies that automate and scale traditional surveillance logics without appropriate legal or ethical oversight (Brayne, 2020; Eubanks, 2018). Moreover, Benjamin (2019) highlighted that empirical studies reveal ongoing issues related to racial bias, wrongful detentions, and declining public trust stemming from these algorithmic systems. This trend underscores a shift from targeted policing to broader forms of social control. The literature emphasizes the importance of algorithmic transparency, protections for civil liberties, and the ethical design of surveillance systems as essential steps to mitigate these negative effects (Couldry & Mejias, 2019; Harcourt, 2015).

### **The Cultural Influence of Police**

The cultural infrastructure of policing institutions greatly influences whether AI reinforces or challenges Hooverist models of surveillance. Research shows that when organizations establish strong norms of justice and accountability, the likelihood of detecting, reporting, and addressing unethical behavior increases significantly (Burrell, Burton, & McGrath, 2023). Conversely, Hooverism's influence continues to cause real harm in departments where ethical values are only aspirational rather than fully embedded in practice. In such settings, AI tools are often used without community consent, leading to wrongful arrests, algorithmic racial bias, suppression of dissent, and growing public distrust (Benjamin, 2019). For example, Haley and Burrell (2025b) described how Detroit's use of facial recognition technology, an AI tool implemented without meaningful public input, resulted in multiple false arrests, disproportionately affecting African American residents. In related work, Haley and Burrell (2024) highlighted how sexual violence and rape disproportionately impact women and racial/ethnic minorities, including American Indian or Alaska Native women and multiracial women, who experience higher victimization rates. They warned that deploying AI driven surveillance and data analysis in law enforcement without transparency and accountability risks reinforcing systemic bias. Such applications may also violate state and federal privacy laws, especially when analytic tools are used without safeguards to ensure fair and lawful outcomes, particularly with sexual assault victims. Additional caution is necessary. The collection and processing of sexual assault victim data often occur without informed consent or proper safeguards, risking the perpetuation of Hooverist information supremacy, in which sensitive personal data, collected, stored centrally, and potentially used or shared either inadvertently or intentionally, can be weaponized under the guise of safety and protection, thus increasing systematic distrust, deepening structural inequalities, and inducing trauma recurrence in victims and vulnerable populations (Haley & Burrell, 2024).

### **AI Dual Use Concerns**

In cases of groundbreaking scientific discoveries in biosecurity and biocybersecurity, AI algorithms can speed up the design and creation of biological agents, such as new pathogens, potent toxins, and genetically modified organisms. A broader institutionalized Hooverist ideology can be mirrored in advanced biomedical research. For example, AlphaFold's ability to predict protein structures now raises dual use concerns. It could be repurposed in a threat scenario to engineer synthetic pathogens with increased virulence and resistance. Experts warn that AlphaFold's predictive power may be exploited when algorithmic tools are freely available without oversight. Malicious actors, including

cybercriminals and state sponsored groups, might bypass current medical defenses and outpace global health response systems (Bloomfield et al., 2024; De Haro, 2024; Haley & Burrell, 2025b; O'Brien & Nelson, 2020), echoing Hooverist themes of expanding technological power justified by preemptive threat narratives, which divert resources and overlook real threats. These risks go beyond traditional cybersecurity issues, exposing deeper weaknesses in the global scientific infrastructure, especially when tools meant for public good are turned toward preemptive control and suppression (Haley & Burrell, 2025b). Viewing AI enabled biothreats through the lens of Hooverism helps scholars and policymakers to go beyond technical fixes and address underlying governance failures, emphasizing transparency, ethical standards, and public oversight to stop the normalization of algorithmic authoritarianism under the pretense of security.

### **Policing Through Prediction**

Empirical studies have identified harms, including bias in AI models and a chilling effect on civil rights. Predictive policing programs, when based on biased historical data, reproduce systemic inequality under the illusion of algorithmic objectivity. In Los Angeles, a well known predictive policing initiative used historical arrest records that disproportionately reflected racialized policing patterns to identify potential crime hotspots (Haley & Burrell, 2025c). This method systematically targeted racially and economically marginalized communities, reinforcing over policing while appearing neutral and data driven. Such practices deepen structural injustices and undermine the legitimacy of policing institutions. As communities see AI as a tool of control rather than protection, public trust declines. The costs are also substantial: investments in costly surveillance technology, along with legal challenges related to civil rights violations, divert resources away from evidence based crime reduction strategies focused on public safety. These entrenched practices reveal how Hoover era frameworks of control still influence modern policing systems. Addressing these issues requires tracing their origins back to the early 20th century, especially J. Edgar Hoover's rise in the 1920s, when policing structures first began to institutionalize exclusionary, racially coded enforcement and centralized data practices, both then and now justified in the language of innovation and national security.

Municipalities across the United States are increasingly investing in expensive AI surveillance technologies, often without enough transparency, oversight, or proven effectiveness. Both urban and rural communities face pressure to adopt so called cutting edge crime prevention tools, including facial recognition systems, predictive policing software, and gunshot detection technologies like ShotSpotter. These systems are often purchased through opaque contracts with private vendors, missing public consultation, proper training, or a clear understanding of the technology's capabilities, limitations, and risks (Haley & Burrell, 2025c).

Unregulated adoption of AI tools exposes communities to various harms, such as ineffective crime reduction, disproportionate targeting, false positives, and misaligned police actions. The growth of public-private surveillance partnerships, especially as federal agencies shrink or privatize, reflects a broader pattern of Hooverism, a commitment to informational dominance justified by technological progress rather than proven results. These trends show how the push for security can override democratic accountability when surveillance becomes routine. Resisting this trend requires renewed focus on civil liberties, public audits, and ethical governance frameworks (Couldry & Mejias, 2019). Participatory policymaking that prioritizes transparency, accountability, and public oversight is vital to ensure AI serves communities rather than controlling them.

## A Critical Reflection on AI Surveillance Infrastructure

In 1976, pioneering computer scientist Joseph Weizenbaum, best known for creating ELIZA and for his critical reflections on AI, described the computer as a metaphor to help us understand what we have done and are doing in a world increasingly shaped by computational logic. His warning about the ethical limits of computing remains resonant today, particularly in the deployment of biometric surveillance technologies. These systems, ranging from facial recognition to fingerprint scanning, embody persistent concerns about the balance between state security and individual rights, as expressed by Hooverists. As Haley (2025b), Marciano (2019) and McKay (2020) have demonstrated, such technologies raise urgent questions about data governance, government overreach, and civil liberties. Grounded historically in Hooverism's pillars of indiscriminate data collection, loyalty enforcement, bureaucratic secrecy, and racialized control, these modern practices perpetuate longstanding patterns of surveillance that disproportionately target marginalized communities while systematically evading public accountability (Almeida et al., 2022; Haley, 2025b; Lewis, 2021). The consequences include the erosion of civil liberties, declining public trust, diminished police legitimacy, and reduced cooperation between communities and law enforcement (Marciano, 2019; Neyland, 2008; Slobogin, 2007).

Evaluating current biometric systems through the Hooverist framework emphasizes the urgent need for transparent and accountable data governance. Without judicial checks, human rights safeguards, or public transparency, biometric technologies risk repeating historical abuses in new technical forms. To address this, applying principles such as informed consent, data minimization, independent audits, and equitable policy frameworks can reduce harm and rebuild public trust (Haley, 2025b; McKay, 2020). Ultimately, recognizing the ideological link between Hoover era surveillance and today's algorithmic policing and automated surveillance techniques allows us to critically examine not only the tools, but also the power structures that support them.

## Theoretical Underpinnings

The fundamentals of surveillance by psychological factors and sociopolitical contexts are not simply a technical matter. As they frame Hooverism as an ideological framework in a system that justifies surveillance, suspicion, and control, these theories uphold Hooverist logic.

### *The Just World Hypothesis*

Melvin Lerner's (1980) just world theory suggests that people tend to believe that individuals get what they deserve. They act out this central belief of an illusion crucial for functioning in a world filled with unavoidable tragedies. This belief, driven by a fear of losing one's own place in the world, contributes to victim blaming, overconfidence in institutions, and rationalization of systemic injustices. These tendencies help to normalize Hooverist ideas, especially against marginalized groups (Hafer & Bègue, 2005). This cognitive bias can stop people from recognizing abuses of surveillance power because they assume only the guilty need to fear. The language of Hooverism, framing surveillance as national security or public safety, exploits this bias by presenting surveillance tools as necessary to maintain social order, while blaming victims by saying they deserve it or are unAmerican, or labeling them national security threats, which reflects just world rationalization. People often accept intrusive privacy violations because they believe these actions target others who must be suspicious. The text shows how terms like *illegal immigrant* or *data subject* dehumanize individuals, creating psychological distance. A suburban voter might support widespread digital surveillance, thinking, "If I am doing nothing wrong, I have nothing to hide." This mindset echoes Hoover's approach of

convincing Americans that surveillance is a neutral tool instead of a political weapon (O'Reilly, 1989; Theoharis, 2004).

### ***Psychological Reactance Theory***

Psychological reactance theory, introduced by Jack Brehm (1966), explains how people experience psychological resistance regarding their behavior. For example, when their freedoms are threatened or restricted, they are motivated to regain them, leading to increased psychological reactance as resistance grows. Instead of discouraging dissent, Hooverism's surveillance tactics sparked a backlash, which amplified public defiance and resistance movements. Outcomes like wrongful arrests or racial bias undermine trust in institutions and fuel civil liberties advocacy. A clear example is the backlash against facial recognition technology used by police departments, where activists argue that such tools violate privacy rights and target marginalized groups. Reactance motivates people to challenge laws, file lawsuits, or organize social movements to reclaim personal and political autonomy. Hooverism's legacy serves as a warning that efforts that attempt total control often produce the very resistance that institutions try to suppress.

### ***The Theory of Proportionality***

Proportionality is a legal and ethical principle stating that government actions, such as surveillance, must be necessary, appropriate, and balanced against the rights they restrict. As a normative tool, it assesses whether governments' pursuits of legitimate goals are justified by the burdens placed on individual freedoms (Barak & Kalir, 2012). Hooverism completely ignored proportionality, favoring unchecked surveillance over individual rights or illegal activities. Today's algorithmic systems often operate invisibly, sweeping across large populations at scale without regard to risk or wrongdoing. For example, deploying drones to monitor a peaceful immigration rally is a disproportionate response, as it suppresses free speech, and using techniques like sting operations, profiling, and broad conspiracy standards generally offers little or no security benefit (Theoharis, 2004). Proportionality theory advocates for using less intrusive methods and emphasizes the democratic need to limit state power.

### ***Social Contract Theory***

Social contract theory emphasizes the mutual relationship between the state and its citizens. It involves justifying the state's authority to protect its people while respecting their rights and freedoms (Hobbes, 1996; Locke, 1980). Hooverism weakens the social contract by expanding surveillance beyond reasonable limits, using algorithmic systems to process personal data without oversight, and lacking transparency in how information is gathered or shared. This erosion of trust undermines the foundation of democratic governance, especially when actions are conducted secretly and without public consent. Hooverism breaches this trust by targeting individuals not for actual criminal activity but for perceived ideological threats. Citizens experience repeated betrayal through modern surveillance when it is used under Hooverism.

### ***Theory of Legitimate and Illegitimate Power***

Social psychologists John French and Bertram Raven (1959) identified six sources of power: legitimate, reward, coercive, expert, referent, and informational. They differentiated legitimate power, which comes from official roles or rules, from illegitimate power, exercised through coercion or manipulation. Legitimate power is considered valid when used openly and aligned with shared norms. Hooverism illustrates the shift from legitimacy to illegitimacy. While J. Edgar Hoover held official authority as FBI Director, his secret,

politically motivated programs like COINTELPRO often crossed legal boundaries, turning into illegitimate influence. For example, Hoover's use of informants on political figures and civil rights leaders gave him coercive power, enabling blackmail and political pressure. Today's equivalents include algorithmic based social credit systems, in which hidden algorithms restrict citizens' opportunities, and unseen predictive hotspot policing. Hooverism demonstrates how institutions can justify surveillance as protective but risk crossing into illegitimate power, undermining democratic trust and accountability.

### ***Organizational Silence Theory***

Morrison and Milliken's (2000) organization silence theory states that collective silence, as a phenomenon, is separate from individual fear and is chosen over speaking out about risks, ideas, or problems that affect innovation, learning, accountability, and ethical outcomes. The reasons people remain silent include fear of retaliation, perceived futility, influence of organizational culture, conflict avoidance, and ambiguity about whether it is appropriate to speak up. Hooverism, as governance through suspicion, explains why whistleblowers were rare during Hoover's reign. Agents or staff who might have objected to racial targeting or ideological surveillance stayed quiet to protect their careers or safety. A modern example is employees in tech companies who hesitate to criticize AI surveillance tools internally, fearing retaliation or being labeled disloyal. Hooverism relies on silence, making organizational silence theory crucial for understanding why unethical surveillance practices often go unchallenged.

### ***Social Learning Theory***

Social learning theory, developed by Albert Bandura (1977), proposes that people learn behaviors through observing, imitating, and modeling others, especially peers and authority figures. Reinforcement and punishment influence whether behaviors are adopted or avoided. Under Hooverism, FBI agents, law enforcement personnel, and government officials are socialized into the institutional culture, normalizing unethical practices as routine and shaping recruits to be ideologically loyal. A current example is law enforcement professionals being pressured to develop surveillance tools without questioning potential misuse. When taught to accept and mimic surveillance practices, modeled behavior becomes institutionalized. Social learning theory explains how Hooverism became a formalized system through modeling and reinforcement, rather than explicit orders alone.

### ***Ethical Climate Theory***

Bart Victor and John B. Cullen (1988) developed ethical climate theory, which states that organizations create dominant ethical environments that influence members' moral reasoning and actions. Climate types include law and code (rule bound), caring (focused on welfare), instrumental (focused on self interest), or independent (focused on individual ethics). Hooverist FBI agents operated in a rules based climate, and often saw loyalty to institutional goals as justification for bending rules or violating personal rights, exemplifying an instrumental environment marked by institutional loyalty and bureaucratic secrecy, shielded from public scrutiny. For example, agents believed that spying on civil rights leaders served the greater good, ignoring legal boundaries and downplaying ethical concerns or the heavy handedness of the 1996 Olympics bombings that ultimately led to a large defamation of character settlement for the wrongly accused, Richard Jewel (Theoharis, 2004). Hao (2025) echoed this in *Empire of AI*, in which modern parallels exist in Silicon Valley, where tech giants have centralized the development and use of AI technologies, wielding disproportionate influence over defense, civil society, and policy without accountability. Ethical climate theory shows how entire organizations can drift into unethical behavior, convinced their actions serve a higher purpose, as seen in the Hooverist

climate that justified secrecy and dominance, revealing how the moral boundaries of power can become dangerously flexible.

### ***Symbolic Interactionism***

Symbolic interactionism, a sociological theory developed by George Herbert Mead and Herbert Blumer (Blumer, 1969), emphasizes the role of social interactions, symbols, and language, which are shaped through interactions in which meaning is modified through interpretation. Hooverism's surveillance became a symbol of control through suspicion. Language shaped through social labeling, such as communist, illegal immigrant, threat, or data subject, illustrates how bureaucratic labels strip individuals of humanity, thereby linking certain behaviors, associations, and appearances to suspicion. These labels are symbols carrying moral weight, justifying surveillance and control, and creating meaning from the top down, embedded in systems. A clear example is how modern algorithmic systems flag suspicious transactions or individuals based on statistical risk scores, reducing complex humans to data points. Symbolic interactionism explains how Hooverism did not just watch people; it also redefined them, enabling widespread acceptance of surveillance as moral and necessary. Today, predictive terms like *suspicion* or *potentially violent* are derived from algorithmic data collected and interpreted by law enforcement and intelligence agencies as indicators of criminal intent in human behavior.

### **Public Private Surveillance Amplifies Systemic Control and Psychological Harm**

Palantir, a data analytics company, offers software widely used by government agencies and private corporations for mass data integration, predictive policing, and immigration enforcement. Using real time surveillance and algorithmic risk assessment, Palantir systems generate algorithmic datadriven risk scores that influence policing and immigration actions. Palantir's Gotham software, originally created for the CIA, was repurposed to incorporate patient data from a healthcare privatization platform developed with Accenture, utilizing the NHS Federated Data Platform, to train predictive models that support immigration enforcement and welfare fraud detection (Borat, 2025). Haggerty (2020) argued that these systems cause stigma and anxiety among those under surveillance, while Benjamin (2019) claimed that predictive policing tools reinforce systemic control and psychological harm, especially in marginalized communities under constant monitoring. These concerns are supported by internal dissent. In 2021, Palantir employees raised ethical objections to the company's role in Immigration and Customs Enforcement, highlighting increased fear and trauma among immigrant populations (Guardian, 2021). A U.S. Government Accountability Office (GAO, 2024) report also revealed a troubling lack of transparency and oversight in these surveillance systems, emphasizing their potential to reinforce systemic bias and worsen psychological stress. Collectively, these developments show how Palantir's technologies continue a form of governance rooted in suspicion and information dominance, extending and deepening the historic Hooverist methods of control.

### **The Systemic Logic of Hooverism**

Hooverism describes a systemic and recursive strategy in which corporate and government actors generate and exploit algorithmic data to consolidate power, often at the expense of human dignity, civil liberties, and democratic accountability. Recent disclosures reveal how companies like Accenture and Palantir, which cohosted the 2024 AI for War conference, stress the need for transnational accountability among for profit corporations, the military, and government entities. As shown in the Accenture Files by Progressive International, Expose Accenture and the Movement Research Unit (2025), Accenture's violations include data extraction, bid rigging, tax evasion, and human rights abuses across 41 contracts. Borat

(2025) highlighted that this amassed data, control, and influence form a dangerous global surveillance infrastructure involving corporations and state actors alike. Additionally, Borat explained that Accenture's financial inclusion tool allows India's Aadhaar program to use, store, transfer, and link the biometric data of 1.3 billion people, but through algorithmic biases, it worsens caste and gender inequalities under a facade of neutrality. Similarly, partnerships between militarized intelligence firms like Palantir show how these repeated patterns keep fueling border militarization and predictive policing.

### **Hooverism and Surveillance Capitalism Intertwined**

Hooverism and surveillance capitalism are distinct but interconnected frameworks that highlight different yet overlapping aspects of modern surveillance. Hooverism focuses on state power, particularly the ideology of surveillance governance established by J. Edgar Hoover's FBI, which used surveillance to enforce political loyalty, racialized control, and bureaucratic secrecy. Hooverism normalized surveillance practices before the digital age, embedding them into intelligence operations and institutionalizing them. Surveillance capitalism (Zuboff, 2019) centers on the market power of corporations that commodify personal data to predict and influence behavior for profit, often without users' consent. It reveals how the normalization of surveillance was monetized and expanded in the digital economy. The importance lies in the combined power of the state and corporate interests, extending Hooverist logic through algorithmic automated decision making means of tracking loyalty, racialized data, and secrecy. This forms the ideological and institutional foundation for suspicion and surveillance capitalism. Together, surveillance capitalism and Hooverism create a dual system of surveillance expansion without consent, in which suspicion (state logic) and profit (corporate logic) reinforce each other.

### **Bias and Social Consciousness Issues**

Racial bias in biometric surveillance technologies reflects a modern form of Hoover surveillance logic, reinforcing systemic inequalities through technology. As Haley (2025b), Conrey and Haney (2024), the ACLU (2023), Lewis (2021), Almeida et al. (2022), Buolamwini (2023), Noble (2018), and Vijeikis et al. (2022) showed, racialized patterns continue in digital systems through biased datasets, targeted actions against racial minorities, and algorithmic decisions that mirror structural discrimination. These practices mirror the core principles of Hooverism: loyalty enforcement, racialized control, informational dominance, and bureaucratic secrecy, by using surveillance as a preemptive tool. This algorithmic governance aligns with philosopher Miranda Fricker's concept of epistemic injustice, in which individuals from marginalized communities are misrepresented or ignored by systems that claim to be neutral and objective (Borat, 2025; Fricker, 2007). Conrey and Haney (2024) emphasized that such misalignments reinforce racial profiling and lead to discriminatory law enforcement actions. Supporting this, the ACLU (2023) and Almeida et al. (2022) highlighted that facial recognition technologies consistently show higher error rates for people of color, increasing the likelihood of false identifications and wrongful arrests. Haley (2025b) and Vijeikis et al. (2022) found that AI training datasets are disproportionately made up of images of white men of European descent, leading to underrepresentation and misclassification of marginalized racial groups. These patterns, viewed through a Hooverist lens, reveal how biometric technologies, lacking ethical safeguards and transparent governance, can automate historical injustices instead of resolving them. To break this cycle, policymakers must incorporate principles of equity, accountability, and participatory oversight into the deployment of surveillance tools.

## Explicit Historical Linkage

The growing body of scholarship on biometric surveillance technologies, as exemplified by Haley (2025b), shows that technical innovations are closely connected to the ideological and institutional roots of Hooverism, which continue through four interconnected pillars: informational supremacy, loyalty enforcement, racialized control, and bureaucratic secrecy. Modern biometric systems, including facial recognition, iris scans, and gait analysis, use advanced AI and sensor technologies under the pretense of crime prediction and violence prevention (Ferguson, 2017; McKay, 2020), yet they replicate entrenched surveillance logics based on state suspicion and social control.

Socially, these technologies raise serious ethical concerns related to privacy breaches, potential misuse, and systemic algorithmic bias, which call for including artificial intelligence within legal frameworks to protect civil liberties (Browning & Arrigo, 2020; Vijeikis et al., 2022). The issues discussed by Haley (2025b), Almeida et al. (2022), and Marciano (2019) mirror priorities similar to Hooverism's focus on extensive government surveillance as a form of social control, leading to institutionalized, broad law enforcement practices that often operate with minimal oversight.

The lack of a clear connection between historical surveillance systems, like Hooverism, and modern algorithmic governance significantly hampers society's ability to understand and address ongoing issues such as racial bias, mission creep, and secrecy in today's biometric surveillance systems. By failing to link contemporary artificial intelligence and biometric technologies used in law enforcement directly with the core principles of Hoover era surveillance, such as unchecked power, systemic racial targeting, and lack of transparency researchers and policymakers risk underestimating how historical legacies continue to fuel deep inequalities today. This oversight restricts the capacity critically to assess and understand embedded biases that shape algorithmic decision making, leading to further mission creep in which surveillance methods expand beyond their original purpose, often without notice or regulation. Therefore, closing this knowledge gap is crucial not only for academic understanding, but also for developing effective policies that address covert continuities (Marshak, 2006) and promote transparency and ethical oversight in algorithmic governance (Almeida et al., 2022; Haley & Burrell, 2025c; Marciano, 2019; Raji & Buolamwini, 2020).

## Insufficient Legal and Ethical Oversight

Automated surveillance technologies and algorithmic policing systems have outpaced existing legal and ethical oversight, demanding urgent attention (GAO, 2023). Recognizing the seriousness of this imbalance requires understanding that AI should not be regarded as routine procurement, in which surveillance tools are heavily funded; instead, it calls for careful and deliberate evaluation of justice and civil liberties (Joh, 2018). EPIC's review of government reports on American Rescue Plan Act expenditures through September 2022 highlighted the extensive and coordinated investment in surveillance infrastructure across the country, from gunshot detection systems funded in Houston, Texas and Hartford, Connecticut to widespread deployment of surveillance cameras in cities like Indianapolis, Indiana, and Springfield, Illinois along with automated license plate recognition systems and drones financed in numerous towns and counties, including Yakima County, Washington and Augusta County, Virginia. Sinha and Trikanad (2023) and Theoharis (2004) supported this Hooverist dependence on informational supremacy, neglecting discriminatory practices by relying on flawed or unvalidated surveillance technologies that can inadvertently continue systematic bias, framing certain neighborhoods or communities as inherently criminal or dangerous, and thus reinforcing negative stereotypes that mirror issues of caste discrimination and automated marginalization through gang databases, facial

recognition errors, and predictive policing hotspots. These interconnected systems, which often produce false positives, can foster a punitive policing model that operates automatically and invisibly. This marks a significant shift in paradigm, illustrating how a Hooverist approach can disproportionately affect marginalized communities and dissenting voices, who may be governed through suspicion alone. Pervasive surveillance can increase psychological stress, anxiety, and fear among residents, deepen social divisions, and undermine the core principles of fairness and justice (Sinha & Trikanad, 2023).

### The Hooverism Framework

The Hooverism framework reimagines surveillance governance by directly challenging the enduring ideological foundations and persistent ideological legacies of Hoover's leadership ideology, namely, informational supremacy, loyalty enforcement, racialized control, and bureaucratic secrecy. These pillars remain embedded in contemporary algorithmic and bureaucratic systems. The framework responds by proposing a six pronged paradigm rooted in democratic accountability, transparency, and human rights. It further incorporates three operational critiques: unchecked power, administrative expediency, and epistemic rigidity to expose how surveillance logic resists scrutiny and perpetuates harm. The accompanying visual illustrates the transformation from Hooverist pillars to democratic governance principles.

Table 1. Hooverist Pillars, Democratic Counter Principles, and Explanation

Hooverist Pillars/ Operational Logics	Democratic Counter Principles	Explanation/Transformation
Informational Supremacy	Data Transparency and Accountability	From secret information dominance to open, reviewable, and accountable data use.
Loyalty Enforcement	Pluralism and Civil Autonomy	From ideological conformity to acceptance of dissent and diversity of thought.
Racialized Control	Equity and Anti Discrimination Safeguards	From targeting and profiling to inclusive, antiracist policy and audit mechanisms.
Bureaucratic Secrecy	Participatory Governance and Transparency	From hidden processes to public deliberation, collaborative governance, and oversight.
Unchecked Power	Legal Restraint and Sunset Clauses	From expanding authority to restrained use, legal oversight, and time limits.
Administrative Expediency	Due Process and Deliberative Pace	From speed over fairness to processes that protect rights and reflect on impact.
Epistemic Rigidity	Critical Reflection and Human Judgment	From treating algorithmic output as truth to emphasizing theoretical, social, and ethical interrogation.

### ***1. Equity as Counterbalance to Racialized Control***

The model emphasizes that surveillance policies must be explicitly crafted to dismantle structural inequalities, especially those that have historically targeted racialized and marginalized communities. Unlike Hooverism's legacy of racialized control (Benjamin, 2019; Theoharis, 2004), equity in surveillance governance calls for demographic impact audits, equity focused algorithms, and targeted redress for communities that have been harmed by discriminatory data practices.

### ***2. Ethics as Antidote to Informational Supremacy***

Where Hooverism promoted the supremacy of unchecked intelligence accumulation, this framework emphasizes the importance of ethical design and practice. Ethical surveillance must be based on democratic values that prioritize consent, proportionality, harm reduction, and the sanctity of civil liberties (Eubanks, 2018; Zuboff, 2019). Moral design principles should be integrated at the programming stage, not added afterward, and they should undergo independent ethical review.

### ***3. Transparency to Dismantle Bureaucratic Secrecy***

To challenge the lasting culture of opacity established under Hooverism, the model requires radical transparency at every stage of data collection, algorithm development, and deployment. This includes publishing publicly available algorithms, mandatory disclosures of surveillance scope and purpose, and accessible records of institutional data use (Haley & Burrell, 2025c). Transparency is crucial not only for public accountability, but also for preventing the normalization of surveillance under administrative neutrality (Monahan, 2006).

### ***4. Stakeholder Engagement to Replace Loyalty Enforcement***

Instead of enforcing loyalty through coercion or institutional gatekeeping, the framework advocates for strong and ongoing stakeholder engagement. Affected communities, civil society groups, technologists, and policymakers participate and collaborate the design and deployment of surveillance governance. Engagement must be institutionalized through participatory design, public deliberation, and community data stewardship models that prioritize the voices of those most affected. As Teo (2024) argued, applying the concept of *slow violence* shows how AI driven surveillance quietly erodes fundamental human rights like privacy, nondiscrimination, and freedom of expression, gradually weakening the human rights framework itself.

### ***5. Oversight as Structural Accountability***

The unchecked surveillance regime promoted by Hooverism flourished largely because of a lack of independent and enforceable oversight mechanisms. This approach advocates creating autonomous oversight bodies with investigative authority, sanctioning power, and public reporting duties. Oversight should go beyond legislative review to include algorithmic audits, human rights evaluations, and ongoing monitoring of unintended effects (Ferguson, 2017; GAO, 2023).

### ***6. Governance Anchored in Democratic Values***

Governance within the Hooverism framework must be grounded in democratic legitimacy, not bureaucratic expediency. This echoes Weizenbaum's (1976) warning that delegating human judgment and moral reasoning to machines is not just misguided, but also potentially fatal. This framework insists that algorithmic decision making must remain subordinate to and within constitutional principles and human oversight, ensuring human

engagements are safeguard, and establishing sunset clauses for all surveillance technologies. Governance should operate under the presumption of restraint, not expansion, of surveillance powers. Upholding the public's right to dissent, privacy, and due process is not optional; it is essential to maintaining democratic accountability in the face of expanding algorithmic authority.

### ***7. Epistemic Rigidity and the Danger of Performance Mode Surveillance***

Finally, the lasting impact of Hooverism stems from Weizenbaum's (1976) epistemological stance of transferring moral judgment and decision making to machines, along with Feigenbaum's framework of computational modes: performance, simulation, and theory. Hooverism illustrates the treatment of information as something actionable and authoritative, representing a dependence on performance mode, in which information is institutionalized as fact. Just as Hooverism used data and dossiers to enforce loyalty and suppress dissent, today's predictive algorithms often skip the cautious approach of simulation or theory in favor of real time action or performance, leaving little space for investigative skills, behavior, syntax, or ambiguity. This epistemic rigidity strengthens both informational and bureaucratic secrecy, creating distance from the truth without accountability through prediction.

### **Framework Summary**

The Hooverism framework not only critiques the historical legacies of ideological surveillance, but also provides a forward looking, principled infrastructure for governing surveillance technologies in an age of algorithmic power. By emphasizing equity, ethics, transparency, stakeholder voice, rigorous oversight, and democratic governance as essential counterweights to Hooverism, the model offers a vital template for reclaiming surveillance from the logics of fear and restoring it to serve justice, dignity, and democratic accountability.

### **Conclusion**

Biometric and algorithmic surveillance systems are now central to both public and private governance, requiring a deliberate shift toward ethical, transparent, and community focused policies. The Hooverism framework acts as an essential intervention that questions the historically rooted ideologies of suspicion, control, and opacity by providing actionable strategies based on democratic principles. This framework highlights equity, ethics, stakeholder involvement, oversight, and governance as crucial pillars to oppose the harmful legacy of Hooverist ideals. By prioritizing these pillars, policymakers and researchers can work toward building surveillance systems that are not only technologically advanced, but also socially fair and accountable to the public.

To implement the Hooverism framework, stakeholders must incorporate structural mechanisms that emphasize transparency, ethics, and bias reduction at every phase of surveillance development and use. Evidence from emerging research highlights the importance of conducting comprehensive impact assessments to evaluate racial and social equity outcomes, ensuring that algorithmic systems do not reinforce historical injustices (Benjamin, 2019; Eubanks, 2018). Policymakers and private entities should enforce mandatory ethical guidelines based on democratic principles, such as proportionality, harm reduction, and safeguarding civil liberties, rather than depending solely on efficiency metrics. Transparency portals and public algorithm registries should be created to facilitate real time oversight by civil society groups, encouraging open communication between developers, affected communities, and regulators. These actions not only help to reduce

bias and opacity, but also foster public trust by making surveillance activities transparent, accountable, and responsive to societal concerns.

Moving forward, the success of this framework depends on sustained interdisciplinary research, collaborative governance, and active community engagement. Silicon Valley's AI technologies form the core of a deeply connected modern empire intertwining government, defense, and society, characterized by concentrated power, secrecy, and control (Hao, 2025). These efforts are vital. Scholars and policymakers should conduct comparative analyses of global surveillance governance models to identify best practices while collaborating on community oversight boards that empower all populations through inclusive education and meaningful participation with a real influence in policy decisions. Legislative reforms must promote algorithmic restraint, human involved checkpoints, and sunset clauses to prevent the unchecked growth of surveillance powers. By focusing on ideology rather than technology in critical inquiry, stakeholders can dismantle the governance logic rooted in suspicion and replace it with systems that uphold justice, dignity, and democratic accountability. Collectively, these strategies position the Hooverism framework as both a conceptual and practical guide for reclaiming surveillance from fear based logics and aligning it with ethical, equitable governance.

## References

Acosta, M., Coronado, D., Ferrández, E., & Moreno, P. J. (2017). Patents and dual-use technology: An empirical study of the world's largest defence companies. *Defence and Peace Economics*, 29(7), 821–839. <https://doi.org/10.1080/10242694.2017.1303239>

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI Ethics*, 2, 377–387.

American Civil Liberties Union. (2023). *How to pump the brakes on your police department's use of Flock's mass surveillance license plate readers*. <https://www.aclu.org/news/privacy-technology/how-to-pump-the-brakes-on-your-police-departments-use-of-flocks-mass-surveillance-license-plate-readers>

Bandura, A. (1977). *Social learning theory*. Prentice-Hall.

Barak, A., & Kalir, D. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139035293>

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. Polity Press.

Bloomfield, D., Pannu, J., Zhu, A. W., Ng, M. Y., Lewis, A., Bendavid, E., Asch, S. M., Hernandez-Boussard, T., Cicero, A., & Inglesby, T. (2024). AI and biosecurity: The need for governance. *Science*, 385(6711), 831–833.

Blumer, H. (1969). *Symbolic interactionism: Perspective and method*. Prentice-Hall.

Borat, E. (2025). The illusion of neutrality: Algorithmic vulnerabilities and corporate-state collusion in the age of surveillance capitalism. *Cyber Defense Review*, 13(2), 17–26.

Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.

Brehm, J. W. (1966). *A theory of psychological reactance*. Academic Press.

Browning, M., & Arrigo, B. A. (2021). Stop and Risk: Policing, Data, and the Digital Age of Discrimination. *American Journal of Criminal Justice*, 46(1), 298–316. <https://doi.org/10.1007/s12103-020-09557-x>

Buolamwini, J. (2023). *Unmasking AI: My mission to protect what is human in a world of machines*. Random House

Burrell, D. N., Burton, S. L., & McGrath, G. E. (2023). Racially Motivated Police Brutality Is a Community Public Health Issue in the United States. *International Journal of Health Systems and Translational Medicine* 3(1), 1-15. <https://doi.org/10.4018/IJHSTM.315296>

Cecil, M. (2014). *Hoover's FBI and the Fourth Estate: The campaign to control the press and the bureau's image*. University Press of Kansas.

Church Committee. (2020). *Cointelpro: An oral history of the FBI's most notorious program*. Lulu Press.

Conrey, C., & Haney, C. (2024). Understanding attitudes toward police surveillance: The role of authoritarianism, fear of crime, and private-sector surveillance attitudes. *Surveillance and Society*, 22, 428–447. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/17177>

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

HALEY: Hooverism as a Framework for Understanding the Historical and Unethical Nature of the Use of Artificial Intelligence and Other Surveillance Practices in the United States

De Haro, L. P. (2024). Biosecurity risk assessment for the use of artificial intelligence in synthetic biology. *Applied Biosafety*, 29(2), 96–107.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.

Foucault, Michel. (1991). Governmentality. In G. Burchell, C. Gordon, & P. Miller (Eds.). *The Foucault effect: Studies in governmentality* (pp. 87–104). University of Chicago Press.

Foucault, Michel. (1995). *Discipline and punish: The birth of the prison*. Trans. Alan Sheridan. Vintage Books.

French, J. R. P., Jr., & Raven, B. (1959). The bases of social power. In D. Cartwright (Ed.), *Studies in social power* (pp. 150–167). Institute for Social Research.

Fricker, M. (2007). *Epistemic Injustice: Power and the Ethics of Knowing* (Oxford, 2007; online edn, Oxford Academic, 1 Sept. 2007). <https://doi.org/10.1093/acprof:oso/9780198237907.001.0001>

Guardian. (2021, March 15). *Palantir whistleblower warns of 'digital panopticon' used by ICE*. <https://www.theguardian.com/technology/2021/mar/15/palantir-ice-whistleblower>

Hafer, C. L., & Bègue, L. (2005). Experimental research on just-world theory: Problems, developments, and future challenges. *Psychological Bulletin*, 131(1), 128–167. <https://doi.org/10.1037/0033-2959.131.1.128>

Haggerty, K. D. (2020). Data-driven disciplinary regimes. *Surveillance & Society*, 18(1), 1–14. <https://doi.org/10.24908/ss.v18i1.13339>

Haley, P. (2025a). Artificial intelligence and ethical dimensions of automated traffic enforcement: Implications for public health, healthcare equity, and social justice. *Health Economics and Management Review*, 6(2), 32–49. <https://doi.org/10.61093/hem.2025.2-03>

Haley, P. (2025b). The impact of biometric surveillance on reducing violent crime: Strategies for apprehending criminals while protecting the innocent. *Sensors*, 25(10), 3160. <https://doi.org/10.3390/s25103160>

Haley, P., & Burrell, D. N. (2024). Leveraging geo-profiling to address rape as a public health and criminal epidemic in the United States. *Land Forces Academy Review*, 29(3), 358–370. <https://doi.org/10.2478/raft-2024-0038>

Haley, P., & Burrell, D. N. (2025a). Artificial intelligence-driven criminal and national security threats in biosecurity, biotechnology, and bio-cybersecurity. *RAIS Journal for Social Sciences* 9(1), 52–72. <https://doi.org/10.5281/zenodo.15428048>

Haley, P., & Burrell, D. N. (2025b). Integrating artificial intelligence into law enforcement: Socioeconomic and ethical challenges. *SocioEconomic Challenges*, 9(2), 60–77. [https://doi.org/10.61093/sec.9\(2\).60-77.2025](https://doi.org/10.61093/sec.9(2).60-77.2025)

Haley, P., & Burrell, D. (2025c). Using artificial intelligence in law enforcement and policing to improve public health and safety. *Law, Economics and Society*, 1(1), 46. <https://doi.org/10.30560/les.v1n1p46>

Hao, K. (2025). *Empire of AI: Dreams and nightmares in Sam Altman's OpenAI*. Penguin Books.

Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age*. Harvard University Press.

Hobbes, T. (1996). *Leviathan* (R. Tuck, Ed.). Cambridge University Press. (Original work published 1651)

Joh, E. E. (2018). Artificial intelligence and policing: First questions. *Seattle University Law Review*, 41, 1139–1146.

Kassler, W. J., & Bowman, C. L. (2023). Overcoming public health “surveillance”: When words matter. *American Journal of Public Health*, 113(8), 1102–1105. <https://doi.org/10.2105/AJPH.2023.307348>

Lerner, M. J. (1980). *The belief in a just world: A fundamental delusion*. Springer.

Lewis, R. (2021). The National Institute of Standards and Technology's role in biometric accuracy. *IEEE Transactions on Emerging Technology*, 13, 222–236.

Locke, J. (1980). *Second treatise of government* (C. B. Macpherson, Ed.). Hackett. (Original work published 1689)

Marciano, Avi. (2019). Reframing biometric surveillance: From a means of inspection to a form of control. *Ethics and Information Technology*, 21, 127–136. [10.1007/s10676-018-9493-1](https://doi.org/10.1007/s10676-018-9493-1).

Marshak, R. J. (2006). *Covert processes at work: Managing the five hidden dimensions of organizational change*. Berrett-Koehler.

McKay, L. (2020). The proliferation of biometric surveillance technologies in modern society. *Journal of Public Policy and Technology*, 16, 151–167.

Monahan, T. (2006). *Surveillance and security: Technological politics and power in everyday life*. Routledge.

Morrison, E. W., & Milliken, F. J. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review*, 25(4), 706–725.

Neyland, D. (2006). *Privacy, surveillance and public trust*. Palgrave Macmillan.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

O'Brien, J. T., & Nelson, C. (2020). Assessing the risks posed by the convergence of artificial intelligence and biotechnology. *Health Security*, 18(3), 219–227.

O'Reilly, K. (1989). *Racial matters: The FBI's secret file on Black America, 1960–1972*. Free Press.

Progressive International, Expose Accenture, & Movement Research Unit. (2025, May 17). PI Briefing No. 18: The Accenture Files. Progressive International. <https://progressiveinternational.org/wire/2025-05-17-pi-briefing-no-18-the-accenture-files/en>

Raji, I. D., & Buolamwini, J. (2020). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society, 429–435. <https://doi.org/10.1145/3375627.3375832>.

Schmid, S., Riebe, T., & Reuter, C. (2022). Dual-use and trustworthy? A mixed methods analysis of AI diffusion between civilian and defense R&D. *Science and Engineering Ethics*, 28, 12. <https://doi.org/10.1007/s11948-022-00364-7>

Sinha, A., & Trikanad, S. (2023). Linking caste and surveillance: How digital governance has legitimised caste discrimination in India. In M. Kwet (Ed.), *The Cambridge handbook of race and surveillance* (pp 76–96). Cambridge University Press.

Slobogin, C. (2007). *Privacy at risk: The new government surveillance and the Fourth Amendment*. University of Chicago Press.

Teo, S. (2024). Artificial intelligence and its 'slow violence' to human rights. *AI Ethics*, 5, 2265–2280. <https://doi.org/10.1007/s43681-024-00547-x>

Theoharis, A. (2004). *The FBI & American democracy: A brief critical history*. University Press of Kansas.

Triola, A. M., & Chanin, J. (2022). Police culture, transparency and civilian oversight: A case study of the National City Police Department. *International Journal of Police Science & Management*, 25(1), 81–95. <https://doi.org/10.1177/14613557221132490>

U.S. Government Accountability Office. (2023). *Facial recognition service: Federal law enforcement agencies should take actions to implement training and policies for civil liberties*. GAO-23-105607. <https://www.gao.gov/products/gao-23-105607>

U.S. Government Accountability Office. (2024). *Facial recognition technology: Federal law enforcement agency efforts related to civil rights and training*. GAO-24-107372. <https://www.gao.gov/products/gao-24-107372>

Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. *Administrative Science Quarterly*, 33(1), 101–125. <https://doi.org/10.2307/2392857>

Vijeikis, R., Raudonis, V., & Dervinis, G. (2022). Efficient violence detection in surveillance. *Sensors*, 22, 2216.

Weizenbaum, J. (1976). *Computer power and human reason: From judgment to calculation*. W. H. Freeman.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.