LUCID TRUTH TECHNOLOGIES®

The Algorithmic Gavel

A Jurisprudential and Operational Analysis of Automated Policing Systems in the United States

Kenneth G. Hartman

Digital Forensics & Cybersecurity Expert

Lucid Truth Technologies

526 West 14th St STE 231

Traverse City, MI 49684

lucidtruthtechnologies.com

231.492.8049

ken@lucid-truth.com

I. Introduction: The Shift from Discretionary to Deterministic Policing

The American criminal justice system is currently navigating a paradigmatic shift of historical magnitude, transitioning from a model of human-centric, discretionary policing to one characterized by algorithmic determinism and automated enforcement. This transformation is not merely a matter of adopting new tools but represents a fundamental restructuring of how the state identifies, investigates, and apprehends citizens. The query regarding the legality of "automated policing"—specifically referencing agentic systems like "Torrential Downpour" alongside traffic cameras and robotic enforcement—touches upon the most volatile intersection of constitutional law and computer science: the delegation of the state's monopoly on force and investigation to non-human agents. Traditionally, the Fourth Amendment's protections against unreasonable searches and seizures were predicated on the intercession of human judgment—the "oath or affirmation" of an officer and the "neutral and detached" review of a magistrate. However, the proliferation of agentic systems, which can operate in an entirely unattended manner, challenges these constitutional safeguards. From peer-to-peer (P2P) surveillance suites that autonomously patrol the internet for contraband to acoustic sensors that dictate police deployment patterns, the operational reality of modern policing is increasingly automated. The legal system has struggled to keep pace, often applying analog precedents to digital realities, resulting in a patchwork of jurisprudence that frequently defers to the opacity of proprietary algorithms. This report provides an exhaustive analysis of this landscape. It examines the operational mechanics and legal standing of specific automated systems, including the P2P monitoring suite "Torrential Downpour," the acoustic gunshot detection system "ShotSpotter," automated warrant generation infrastructures, and the nascent field of autonomous physical enforcement via robotics and vehicles. Through this analysis, a central thesis emerges: while "fully automated" arrests (where no human is involved at any stage) remain legally aspirational

rather than actual, the current system functions as a "rubber stamp" regime. In this regime, the machine generates the probable cause or reasonable suspicion, and the human legal actors—officers, prosecutors, and judges—serve primarily to ratify the algorithm's conclusions, often without the technical capacity to scrutinize the "black box" driving the enforcement action.

II. Agentic Surveillance in the Digital Domain: The Case of Torrential Downpour

The most sophisticated implementation of automated policing currently deployed in the United States is found not on the streets, but in the digital ether. The software suite known as "Torrential Downpour" serves as the primary case study for "agentic systems that trigger an arrest".[1] Unlike passive surveillance tools that simply record events, Torrential Downpour is active, intrusive, and capable of autonomous investigative workflows that rival human detectives in complexity and exceed them in scale.

2.1 The Operational Mechanics of Automated P2P Investigations

Torrential Downpour is a proprietary forensic software tool used by federal agencies, including the FBI and DHS, as well as local law enforcement, to monitor BitTorrent peer-to-peer networks.[2] It is often part of a broader software suite known as "RoundUp," which includes various applications designed to conduct highly intrusive digital surveillance across different file-sharing protocols.[4] The system's automation is its defining feature. It allows law enforcement to patrol the vast expanse of P2P networks without constant human supervision. The software is configured to search for "hash values"—unique 32-digit alphanumeric codes that serve as digital fingerprints for specific files.[5] When a user shares a file on a BitTorrent network, they are not sharing the file itself but offering it to the "swarm." Torrential Downpour acts as a peer in this swarm. It does not merely observe; it actively participates in the network handshake protocols. As detailed in federal court filings, such as those in *United States v. Gonzales* and *United States v. Vos* , the software performs a sequence of automated tasks:

> **Autonomous Scanning:** The software scans the network for IP addresses advertising

files with hash values known to match Child Sexual Abuse Material (CSAM) or other illicit content.[3]

> **The Handshake and Download:** Upon detecting a target, the software initiates a connection. It is designed to force a "single-source download" from the specific IP address associated with the suspect, ensuring that the data packets received can be mathematically linked to that specific user rather than the collective swarm.[2]
>
> **Data Logging:** It automatically logs the date, time, IP address, port identifier, and the specific file paths and names shared by the target computer.[5]

Automated Referral: Perhaps most critically for the concept of "automated policing," the software can be integrated with databases like the Child Protection System (COPS). Agents can set parameters to "automatically request leads" from COPS based on the IP addresses detected by Torrential Downpour.[7]

This workflow demonstrates that the system works in an entirely unattended manner during the critical investigative phase. The software identifies the crime, collects the evidence, verifies the suspect's digital identity, and prepares the referral for the human agent. The agent's role is frequently reduced to reviewing the automated log and signing the affidavit—a process that raises profound questions about the "Oath or affirmation" clause when the affiant has no personal knowledge of the events other than what the machine reports.

2.2 The Fourth Amendment and the "Public" Nature of P2P

The legality of Torrential Downpour has been challenged repeatedly on Fourth Amendment grounds, specifically arguing that the software conducts an unreasonable warrantless search of a user's computer. However, federal courts have largely established a permissive framework for this form of automated policing, relying on the "Third Party Doctrine" and the public nature of P2P file sharing. The prevailing judicial view, articulated in cases such as *United States v. Weast* and confirmed in district rulings involving Torrential Downpour, is that a user has no reasonable expectation of privacy in files they voluntarily share on a peer-to-peer network.[2] When a user installs BitTorrent software and configures a folder for sharing, they are broadcasting their IP address and file list to the world. The court in *United States v. Neiheisel* noted that the software "cannot access non-public areas or unshared portions of an investigated computer," nor can it override settings on a suspect's computer.[5] Therefore, the automated interaction initiated by Torrential Downpour is legally equivalent to an undercover officer buying drugs from a street dealer who openly offers them for sale. The fact that the "officer" is a script running on a server in a data center does not alter the constitutional analysis under current doctrine. The automation merely scales the "plain view"

observation to a level impossible for human agents to achieve manually.[5]

2.3 The "Black Box" Discovery Disputes and Due Process

While the Fourth Amendment challenges have largely failed, a significant legal battleground has emerged regarding Due Process and the right to a fair trial: the "Black Box" problem. Defense attorneys argue that if the government relies on an automated system to generate the sole evidence for an arrest, the defense must be allowed to

inspect the "accuser"—in this case, the source code of Torrential Downpour.[3] In *United States v. Clarke* , the Second Circuit addressed this issue directly. The defendant sought discovery of the Torrential Downpour software and its source code to test its reliability and potential for error (e.g., hash collisions or IP spoofing). The government resisted, arguing that disclosing the source code would compromise the tool's efficacy and allow criminals to reverse-engineer it.[1] 3 The court sided with the government, ruling that the defense had not made a sufficient showing of irregularity to warrant piercing the "law enforcement privilege" that protects proprietary investigative tools.[1] 4 This creates a legal asymmetry. The automated system is presumed reliable, and its output (the log file) is admitted as a business record. The defendant is denied the tools necessary to challenge the internal logic of the automation. Expert witnesses for the defense, such as those in *United States v. Budziak* , have argued that without access to the software, they cannot "impeach the reliability of computer evidence," effectively denying the defendant the right to cross-examine the witness against them.[3] This reinforces the "rubber stamp" dynamic: the court relies on the machine's output because the mechanism of the machine is legally shielded from scrutiny.[15]

Table 1: Comparative Analysis of Automated Digital Forensic Tools

System Name	Functionality	Automation Level	Legal Status / Key Precedents
Torrential Downpour	P2P Monitoring & Hash Verification	**High:** Auto-scans, auto-downloads, auto-refers to COPS database.[7]	Upheld under “Plain View” doctrine; Source code privileged (*US v. Clarke*). [5]
RoundUp	Suite of P2P monitoring tools	**High:** Manages multiple surveillance applications simultaneously.[4]	Broadly used; challenges focus on specific modules like Torrential Downpour.[4]
Peer Spectre	List Generation of Sharers	**Medium:** Produces lists of IP addresses sharing CSAM for warrants.[10]	Output accepted as “substantial basis” for probable cause (*US v. Thomas*).[10]
Hyphanet Tools	Darknet/I2P Monitoring	**High:** Penetrates anonymized networks.	**Contested:** Canadian courts have excluded evidence due to misleading warrant applications regarding the tool’s capabilities.[16]

III. Acoustic Panopticism: ShotSpotter and the Fabrication of Suspicion

While Torrential Downpour automates the investigation of digital contraband, the "ShotSpotter" system (now branded as SoundThinking) attempts to automate the detection of physical violence. This technology illustrates the friction between automated alerts and the constitutional standard of "Reasonable Suspicion," highlighting the dangers of "automation bias" in street-level policing.

3.1 The Illusion of Human Review

ShotSpotter deploys networks of acoustic sensors in urban environments to detect and triangulate the sound of gunfire. The system is marketed as a "precision policing" tool that bypasses the need for 911 calls. The company claims a rigorous "human-in-the-loop" process wherein an algorithm detects a sound, classifies it, and sends the audio clip to a review center where a human acoustic analyst confirms the classification before dispatching police.[17] However, investigative reporting and legal discovery have revealed that this human review is often perfunctory, serving more as a liability shield than a genuine quality control measure. Internal documents obtained by the Associated Press describe a "WARNING: CONFIDENTIAL" operations manual that instructs reviewers to look for audio patterns resembling a "sideways Christmas tree".[18] More alarmingly, human employees can—and do—overrule the algorithm's rejection of a sound. In roughly 10% of cases, humans reverse the machine's determination, sometimes classifying sounds as gunshots that the algorithm initially dismissed as fireworks or thunder.[1] 8 Furthermore, there is evidence of "post-hoc fabrication" of evidence. In several cases, police departments have contacted ShotSpotter after an incident to ask if the system "missed" a shot. Analysts have then manually reclassified previously dismissed sounds (like fireworks) as gunshots to align with the police narrative, creating retroactive probable cause.[18] This fundamentally undermines the objectivity of the automated system, turning it into a tool for confirmation bias rather than independent detection.

3.2 From Algorithm to Reasonable Suspicion: The Rickmon Precedent

The legal implications of ShotSpotter alerts are profound, particularly regarding the Fourth Amendment's regulation of *Terry* stops (investigative detentions). The central legal question is whether an automated alert, which has a known error rate and is often triggered by non-criminal sounds (fireworks, construction noise), can constitute the "specific and articulable facts" required to stop and frisk a citizen. The Seventh Circuit's

decision in *United States v. Rickmon* sets a pivotal and controversial precedent. The court held that a ShotSpotter alert, combined with a vehicle's presence in the vicinity of the alert and the officer's observation of the vehicle departing the area, provided sufficient reasonable suspicion for a stop.[1] 9 This ruling effectively automates the generation of reasonable suspicion. An officer no longer needs to hear the shot or see the weapon; they need only receive a digital notification on their terminal. This creates a "feedback loop of suspicion." ShotSpotter sensors are disproportionately

deployed in low-income, minority neighborhoods.[20] Because the sensors are there, they generate alerts. Because there are alerts, police treat the area as a "high-crime zone" (a factor in Fourth Amendment analysis). This designation lowers the threshold for future stops, justifying further aggressive policing. Critics argue that this creates a technological veneer for racial profiling, where the "objective" machine provides the legal cover for practices that would otherwise be unconstitutional.[2] 0

3.3 The "Ears in the Sky" and Privacy

Beyond the immediate seizure of persons, acoustic gunshot detection systems raise privacy concerns regarding the recording of conversations. While the NYPD and ShotSpotter policy state that sensors are "not designed to pick up human voices," independent testing and court cases have shown that they can and do record intelligible speech.[1] 9 In *People v. Johnson* , a California court admitted a recording of a verbal altercation captured by ShotSpotter as evidence of a homicide.[19] This capability transforms the system from a gunshot detector into a generalized acoustic surveillance grid. The "plain view" (or "plain hearing") doctrine protects these recordings if the conversation occurs in a public space where there is no expectation of privacy. However, the persistence and ubiquity of the sensors create a "mosaic" of surveillance that some legal scholars argue should trigger Fourth Amendment protection, similar to the reasoning in *Carpenter v. United States* regarding cell site location data.[19]

IV. Biometric Determinism: Facial Recognition and the "Oath"

Facial Recognition Technology (FRT) represents the shift from investigating a specific suspect to investigating the entire population. The integration of FRT into policing workflows highlights the danger of "automation bias"—the cognitive tendency of humans to trust automated decision support systems over contradictory evidence—and how this bias infects the warrant application process.

4.1 Automation Bias and the Case of Robert Williams

The most prominent example of the failure of automated biometric policing is the wrongful arrest of Robert Williams in Detroit. Williams was arrested in front of his family and detained for 30 hours based solely on a match generated by an FRT algorithm that incorrectly identified him as a shoplifting suspect captured on grainy CCTV footage.[23] When detectives interrogated Williams, they presented the photo from the CCTV and the FRT match. Williams immediately pointed out that the person in the video was not him. The detective, displaying classic automation bias, reportedly replied, "The computer says it's you".[2] 4 This incident reveals that for many officers, the algorithm is not merely an investigative lead; it is a truth-teller that overrides their own sensory perception. The Detroit Police Chief later admitted that "the computer got it wrong" and that the arrest was the result of "poor investigative work".[25] However, this "poor work" is a systemic feature of introducing probabilistic algorithms into a high-pressure legal environment. Officers are incentivized to close cases, and a "match" from a sophisticated software system provides a psychological and administrative shortcut to probable cause.[26]

4.2 The Constitutional Friction: "Investigative Leads" vs. Probable

Cause Law enforcement agencies consistently argue in policy documents that FRT results are only "investigative leads" and do not constitute probable cause for arrest.[2] 5 However, the Williams case and others demonstrate that in practice, the FRT match becomes the probable cause. Officers often use the FRT match to construct a photo lineup, which is then shown to a witness (who may be influenced by the same bias), or they simply write an affidavit stating that the suspect was "identified" via investigative means, obscuring the role of the algorithm from the magistrate.[24] This practice fundamentally erodes the "Oath or affirmation" clause of the Fourth Amendment. When an officer swears that they have probable cause to arrest a suspect based on a computer match they have not independently validated, they are swearing to the accuracy of a "black box" they do not understand. This has led to legislative pushback. For instance, West Virginia's proposed "Responsible Use of Facial Recognition Act" explicitly legislates the Fourth Amendment standard into the technology, stating that "no warrant shall issue" based solely on FRT results without corroborating evidence.[28] This type of legislation attempts to force the "human loop" back into the system by statute, acknowledging that the operational inertia of automated policing tends to bypass it.

V. The Administrative Automaton: Warrants, Robo-Signing, and "Dirty Data"

Perhaps the most pervasive form of automated policing is not a robot on the street or a scanner on the web, but the silent, bureaucratic automation of the warrant and court record systems. This "administrative automaton" governs the issuance of arrest warrants and the management of criminal records, often with devastating efficiency and minimal oversight.

5.1 The Automated Warrant Pipeline

Modern court and police systems are increasingly integrated to automate the issuance of warrants for "Tier I" offenses and failure-to-appear violations. In states like Ohio and Colorado, task forces have recommended or implemented systems where warrants are automatically entered into the Law Enforcement Automated Data System (LEADS) and the National Crime Information Center (NCIC) within 48 hours of issuance.[2] 9 The "Automated Court Date Reminder" studies show that technology can reduce warrants by reminding defendants to appear, but the punitive side of the automation remains robust.[3] 1 When a defendant misses a court date, case management software can automatically trigger the generation of a bench warrant. This digital "arrest order" propagates instantly to police cruisers via the NCIC database.

5.2 "Dirty Data" and the Herring Exception

The reliance on these automated databases introduces the problem of "dirty data"—incorrect, stale, or rescinded warrants that remain in the system. In *Herring v. United States* , the Supreme Court addressed whether evidence found during an arrest based on a warrant that had been recalled months earlier—but remained in the computer system due to clerical error—should be suppressed. The Court ruled that it should not , creating a "good faith" exception for reliance on negligent record-keeping.[3] 2 This ruling creates a perverse incentive structure. It reduces the pressure on agencies to

maintain clean data. If an automated system erroneously indicates a warrant exists, and an officer acts on it, the resulting arrest and any evidence found (e.g., drugs in the suspect's pocket) are legally valid. The automation of the warrant system, therefore, expands the police power to seize citizens based on administrative errors that are insulated from the exclusionary rule.[33]

5.3 "Robo-Signing" and the Rubber Stamp Magistrate

The term "robo-signing," infamous from the 2010 mortgage foreclosure crisis, has migrated to the criminal justice system. It refers to the practice of affiants (officers or clerks) signing hundreds of affidavits per day without reading them or verifying the underlying facts, often using automated templates.[3] 4 In the context of automated traffic enforcement and debt collection lawsuits, this practice is rampant. Officers are often presented with a stack of citations generated by red-light cameras or speed cameras. State laws, such as those in Florida, require an officer to "review" the infraction. However, in practice, this review is often a split-second click to confirm the machine's finding.[3] 6 This "rubber stamping" extends to the judiciary. Studies of warrant applications suggest that magistrates often approve warrants in less time than it takes to read the affidavit, relying on the "formatted" nature of the request. When the request is generated by a trusted system (like Torrential Downpour or a traffic camera), the judicial check becomes a formality, effectively delegating the judicial power to the software that prepared the document.[3] 8

VI. Physical Agency: Robotics, Autonomous Vehicles, and the Future of Force

The inquiry regarding "agentic systems that trigger an arrest" finds its most literal interpretation in the emerging field of physical robotics and Autonomous Vehicles (AVs). Here, the "agent" is not just software but a physical entity capable of exerting control over physical space and human bodies.

6.1 The Robotic "Terry" Stop and Use of Force

Current deployments of police robots, such as Knightscope's K5, are primarily surveillance platforms—"cameras on wheels" that patrol malls and parking lots.[40] However, legal scholars and privacy advocates warn that the functional capabilities of these robots are expanding toward active enforcement. A critical legal question is whether a robot can conduct a *Terry* stop. If a robot blocks a pedestrian's path and issues a command—"Halt, you are being recorded, stay where you are"—and a reasonable person would not feel free to leave, a Fourth Amendment seizure has occurred.[4] 2 The robot effectively detains the suspect until human officers arrive. This "robotic detention" raises liability questions: If the robot malfunctions and injures the suspect, or if the detention is based on a facial recognition error, who is liable? The manufacturer? The deploying agency? The software developer? The use of lethal force by robots has already occurred. In 2016, the Dallas Police Department used a Remotec

Andros robot to deliver an explosive charge to kill a sniper who had murdered five officers.[4] 3 While this robot was remote-controlled, it set a precedent for the robotic delivery of lethal force. There are currently no federal laws explicitly prohibiting autonomous robots from using force, though the debate over "Lethal Autonomous Weapons Systems" (LAWS) is active in international law and domestic policy circles.[44]

6.2 Autonomous Vehicles as Policing Agents

The widespread adoption of Autonomous Vehicles (AVs) presents two novel scenarios for automated policing:

> **The Kill Switch (Remote Seizure):** As vehicles become connected to municipal networks, the technical capacity for law enforcement to remotely disable a vehicle exists. A "digital roadblock"—where an algorithm identifies a fleeing or stolen vehicle and transmits a "stop" command—would constitute a seizure under the Fourth Amendment.[4] 6 Legal frameworks are currently underdeveloped, but the "exigent circumstances" doctrine would likely be stretched to justify such automated seizures to prevent high-speed chases.
>
> **The Vehicle as Informant:** AVs are laden with sensors (LiDAR, cameras) that record their surroundings. Police agencies are increasingly viewing these vehicles as mobile surveillance nodes. An AV could, theoretically, be programmed to automatically report traffic violations it observes (e.g., a speeding car passing it) or to scan license plates and

alert the police cloud.[4] 8 This would effectively deputize the entire transportation grid, creating a panopticon where the observer is the car next to you.

VII. Computational Law and the Era of Smart Contracts

The ultimate evolution of automated policing is "Computational Law"—a legal theory where the law is not just enforced by code but is the code.

7.1 Smart Contracts and "Self-Help" Enforcement

In the financial sector, "Smart Contracts" on blockchain platforms are already automating the execution of legal penalties. If a borrower misses a payment, the contract automatically executes a penalty or transfers collateral.[5] 0 Applied to policing, this concept envisions systems where a violation triggers an immediate, automated sanction without human intervention. For example, "smart" infrastructure could detect a speeding vehicle and automatically deduct the fine from the driver's digital wallet. If

the wallet is empty, the system could digitally "boot" the car. This creates a system of "perfect enforcement" that lacks the procedural due process of a hearing or the opportunity for an officer to exercise discretion (e.g., not ticketing a speeding driver rushing to the hospital).[3] 8

7.2 Suspicious Activity Reports (SARs) as Automated Freezing

A current analog to this is the Suspicious Activity Report (SAR) regime. Financial algorithms monitor transactions for patterns indicative of money laundering. When a threshold is breached, a SAR is automatically generated and filed with FinCEN.[5] 3 While a SAR is not an arrest, it often leads to the immediate, automated freezing of accounts by the bank to mitigate risk. This effectively seizes a citizen's property based on an algorithmic "suspicion" score, often leaving them with little recourse to challenge the "black box" that flagged them.[54]

Unlike the European Union, which offers protection under GDPR Article 22 against decisions based "solely on automated processing," the United States lacks a comprehensive federal statute protecting citizens from these automated legal adjudications. This leaves American citizens uniquely vulnerable to a justice system where the accuser, the witness, and the executioner are all lines of code.[5] 6

VIII. Synthesis: The Matrix of Automated Control

The operational reality of automated policing in the United States is best understood not as a collection of isolated gadgets, but as a three-tiered matrix of control that is progressively removing human friction from the machinery of justice.

8.1 The Three Layers of Automation

The Sensor Layer (Data Collection): This layer is ubiquitous and passive. It includes ShotSpotter sensors, traffic cameras, AV telemetry, and the "plain view" monitoring of P2P networks by tools like Torrential Downpour. These systems create the "haystack" of data.[17]

The Agentic Layer (Analysis & Lead Generation): This is the layer of active intelligence. Software like Torrential Downpour doesn't just watch; it interacts, verifies hashes, and creates leads. FRT algorithms process faces. Predictive policing algorithms like PredPol (Geolitica) identify "hot spots." This layer converts raw data into "suspicion".[7]

The Bureaucratic Layer (Execution): This is the layer of legal authority. Automated warrant databases (NCIC), robo-signed affidavits, and smart contracts convert the "suspicion" generated by the agentic layer into "force"—an arrest warrant, a frozen account, or a seized vehicle.

8.2 The Erosion of the "Oath"

The profound legal casualty of this matrix is the Fourth Amendment's requirement for an "Oath or affirmation." The Founders envisioned a system where a human being staked their reputation and liberty on the truth of their accusations. In the automated regime, the "accuser" is an algorithm protected by trade secrets. The human officer who signs the

warrant is often merely attesting to what the computer told them. This "hearsay of the machine" insulates the entire process from accountability. If the machine errs—as in the case of Robert Williams or the thousands of false ShotSpotter alerts—the system shrugs. The officer acted in "good faith" reliance on the technology, and the technology is proprietary.

Table 2: Legal Vulnerabilities of Automated Policing Systems

System Type	Primary Legal Defense Challenge	Fourth Amendment Status	Future Outlook
P2P Surveillance (Torrential Downpour)	Source Code Secrecy / Validation	**Permitted:** No Expectation of Privacy in Public IP (*Weast*).	Continued expansion; encryption is the only barrier.
Gunshot Detection (ShotSpotter)	Reliability / Automation Bias	**Permitted:** Generates Reasonable Suspicion (*Rickmon*).	High litigation risk; questions of “manufactured” suspicion.
Facial Recognition	Racial Bias / Wrongful Identification	**Contested:** “Investigative Lead” vs. Probable Cause.	Likely to face strict statutory regulation (e.g., WV SB 688).
Automated Warrants	Data Hygiene (Stale Warrants)	**Permitted:** Good Faith Exception (*Herring*).	Integration with AI to predict flight risk/recidivism.
Traffic Automation	Due Process (Burden Shifting)	**Civil/Admin:** Generally upheld if human review exists.	Expansion to “noise cameras” and “distracted driving” AI cameras.

System Type	Primary Legal Defense Challenge	Fourth Amendment Status	Future Outlook
Robotic/AV Enforcement	Definition of “Seizure” / Use of Force	**Unsettled:** No clear precedent for autonomous use of force.	Legislative vacuum; policy will likely precede case law.

In conclusion, "automated policing" is not a future possibility; it is the current operating system of American law enforcement. From the P2P swarms monitored by Torrential Downpour to the streets listened to by ShotSpotter, the "agentic system" has arrived. It works in an unattended manner to identify crime, and while it may not yet physically handcuff a suspect without a human present, it constructs the digital cage from which the suspect cannot escape. The challenge for the American legal system is whether it can adapt its 18th-century protections to a 21st-century reality where the constable is a code.

Works Cited

1. Tracking Child Pornography with Torrential Downpour | Tulsa Sex Crimes Defense Lawyer, accessed November 18, 2025, https://www.defendingtulsa.com/video/tracking-child-pornography-with-torrenti
2. USA v. Ewing, No. 24-11308 (11th Cir. 2025) - Justia Law, accessed November 18, 2025, https://law.justia.com/cases/federal/appellate-courts/ca11/24-11308/24-11308-202
3. RECEIVED - Wisconsin Court System - Log in to Wisconsin eCourts, accessed November 18, 2025, https://acefiling.wicourts.gov/document/eFiled/2019AP001983/252222
4. Challenging Digital Evidence Obtained through RoundUp and Torrential Downpour - NACDL, accessed November 18, 2025, https://www.nacdl.org/Content/Webinar-Challenging-Digital-Evidence-Obtained-
5. LAWRENCE YOUNGMAN vs STATE OF FLORIDA :: 2022 - Justia Law, accessed November 18, 2025, https://law.justia.com/cases/florida/second-district-court-of-appeal/2022/21-2472
6. Amicus Curiarum - Maryland Courts, accessed November 18, 2025, https://www.courts.state.md.us/sites/default/files/amicus-curiarum/201903amicus
7. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 WO IN THE UNITED STATES DISTRICT COURT FOR THE DISTRI - GovInfo, accessed November 18, 2025, https://www.govinfo.gov/content/pkg/USCOURTS-azd-2_17-cr-01311/pdf/USCOU
8. Case 2:17-cr-01311-DGC Document 86 Filed 08/27/19 Page 1 of 17 - GovInfo, accessed November 18, 2025, https://www.govinfo.gov/content/pkg/USCOURTS-azd-2_17-cr-01311/pdf/USCOU
9. Surveillance Technologies and Constitutional Law - PMC - PubMed Central - NIH, accessed November 18, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10704392/
10. Fiore v. United States of America, No. 2:2023cv00220 - Document 2 (D. Vt. 2025) :: Justia, accessed November 18, 2025, https://law.justia.com/cases/federal/district-courts/vermont/vtdce/2:2023cv00220
11. The Informer: March 2020 - Federal Law Enforcement Training Centers, accessed November 18, 2025, https://www.fletc.gov/sites/default/files/informer/2020-12/3informer20.pdf

12. Peer-to-Peer File Sharing Case Law Review - Locate the Law, accessed November 18, 2025, https://locatethelaw.org/wp-content/uploads/2024/05/Peer-to-Peer-Case-Law.p
13. Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials - Mass.gov, accessed November 18, 2025, https://www.mass.gov/doc/electronic-evidence-in-criminal-investigations-and-ac
14. Second Circuit Reaches for Affirmance in Child Pornography Case, accessed November 18, 2025, https://www.pbwt.com/second-circuit-blog/second-circuit-reaches-for-affirman
15. Case: 4:16-cr-00374-JAR Doc. #: 63 Filed: 08/25/17 Page: 1 of 40 PageID - GovInfo, accessed November 18, 2025, https://www.govinfo.gov/content/pkg/USCOURTS-moed-4_16-cr-00374/pdf/USC
16. Hyphanet - Wikipedia, accessed November 18, 2025, https://en.wikipedia.org/wiki/Hyphanet
17. Police Technology: Acoustic Gunshot Detection Systems - Illinois Criminal Justice Information Authority, accessed November 18, 2025, https://icjia.illinois.gov/researchhub/articles/police-technology-acoustic-gunshot-
18. Confidential document reveals key human role in gunshot tech | AP News, accessed November 18, 2025, https://apnews.com/article/shotspotter-artificial-intelligence-investigation-9cb47
19. EARS IN THE SKY: HOW THE TECHNOLOGY OF SHOTSPOTTER IS ERODING FOURTH AMENDMENT PROTECTIONS - Capital University Law Review, accessed November 18, 2025, https://www.capitallawreview.org/api/v1/articles/55609-ears-in-the-sky-how-the-
20. The Dangers of Automated Gunshot Detection - Penn Carey Law: Legal Scholarship Repository, accessed November 18, 2025, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1022&context=jli
21. "The Automated Fourth Amendment" by Maneka Sinha - Emory Law Scholarly Commons, accessed November 18, 2025, https://scholarlycommons.law.emory.edu/elj/vol73/iss3/2/
22. SHOTSPOTTER: IMPACT AND USE POLICY - NYC.gov, accessed November 18, 2025, https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/sh
23. How Face Recognition Technology Landed One Innocent Man in New Jersey Jail for Ten Days, accessed November 18, 2025, https://www.aclu-nj.org/news/how-face-recognition-technology-landed-one-inn
24. The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest - Washington and Lee University School of Law Scholarly Commons, accessed November 18, 2025, https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4773&context=
25. The Civil Rights Implications of the Federal Use of Facial Recognition Technology, accessed November 18, 2025, https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf
26. Facial Recognition Technology U.S. Commission on Civil Rights 1331 Pennsylvania Ave. - ACLU, accessed November 18, 2025, https://www.aclu.org/wp-content/uploads/2024/04/ACLU-Comment-to-USCCR-r
27. How regulators can get facial recognition technology right | Brookings, accessed November 18, 2025, https://www.brookings.edu/articles/how-regulators-can-get-facial-recognition-te
28. SB 688 Text - West Virginia Legislature, accessed November 18, 2025, https://www.wvlegislature.gov/Bill_Status/bills_text.cfm?billdoc=sb688%20intr.htm
29. Automating Arrest Warrants Between Courts and Law Enforcement, accessed November 18, 2025, https://www.ojp.gov/ncjrs/virtual-library/abstracts/automating-arrest-warrants-be
30. Warrant Reform Recommendations Released - Governor Mike DeWine - Ohio.gov, accessed November 18, 2025, https://governor.ohio.gov/media/news-and-media/053119
31. Automated Court Date Reminders Reduce Warrants for Arrest: Evidence from a Text Messaging Experiment - Journal Article - Stanford Law School, accessed November 18, 2025, https://law.stanford.edu/publications/automated-court-date-reminders-reduce-

32. GAO-02-716 Welfare Reform: Implementation of Fugitive Felon Provisions Should Be Strengthened, accessed November 18, 2025, https://www.gao.gov/assets/gao-02-716.pdf
33. Good Faith Exception to the Exclusionary Rule in North Carolina - Powers Law Firm PA, accessed November 18, 2025, https://www.carolinaattorneys.com/blog/good-faith-exception-exclusionary-rule-
34. “Robo-Signing” and Other Alleged Documentation Problems in Judicial and Nonjudicial Foreclosure Processes - EveryCRSReport.com, accessed November 18, 2025, https://www.everycrsreport.com/reports/R41491.html
35. Consumer Credit Cases and Robosigning | Creedon & Gill P.C., accessed November 18, 2025, https://www.creedongill.com/blog/2021/07/consumer-credit-cases-and-robosigni
36. How to Beat a Red Light Camera Ticket in Florida – A Guide - Ticket, accessed November 18, 2025, https://www.ticketshield.com/es/insights/how-to-beat-red-light-camera-ticket-fl
37. Red Light Camera Safety Program - Pinecrest-FL.gov, accessed November 18, 2025, https://www.pinecrest-fl.gov/Government/Police/Red-Light-Camera-Safety-Prog
38. Observing the Effects of Automating the Judicial System with Behavioral Equivalenc - Scholar Commons, accessed November 18, 2025, https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4427&context=sclr
39. On Warrants & Waiting: Electronic Warrants & The Fourth Amendment - Digital Repository @ Maurer Law, accessed November 18, 2025, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11513&context
40. Can a robot be racist? - Mike Walsh, accessed November 18, 2025, https://www.mike-walsh.com/blog/can-a-robot-be-racist
41. Policing Police Robots - UCLA Law Review, accessed November 18, 2025, https://www.uclalawreview.org/policing-police-robots/
42. Terry in the Age of Automated Police Officers - eRepository @ Seton Hall, accessed November 18, 2025, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1734&context=shlr
43. Robert Sassan, Civil Liability for Autonomous Police Robots: The Inadequacy of § 1983 in Responding to - Richmond Journal of Law and Technology, accessed November 18, 2025, https://jolt.richmond.edu/files/2024/04/Sassan-JOLT-Final-4-12.pdf
44. Matthew Tokson* - Penn Carey Law: Legal Scholarship Repository, accessed November 18, 2025, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1904&context=jcl
45. Proposed Rules to Determine the Legal Use of Autonomous and Semi-Autonomous Platforms in Domestic U.S. Law Enforcement - Carolina Law Scholarship Repository, accessed November 18, 2025, https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1362&context=ncjolt
46. Automated Seizures: Police Stops of Self-Driving Cars - NYU Law Review,
47. Identifying High-Priority Needs for Law Enforcement Interactions With Autonomous V - RAND, accessed November 18, 2025, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA108-
48. Autonomous vehicles: The legal landscape in the US | Publications | Knowledge | Global law firm, accessed November 18, 2025, https://www.nortonrosefulbright.com/en/knowledge/publications/2951f5ce/auton
49. AUTOMATED SEIZURES: POLICE STOPS OF SELF-DRIVING CARS - NYU Law Review, accessed November 18, 2025, https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULawReview-94-J
50. Virtual Hearings and Blockchain Technology Solutions in Criminal Law - Mitchell Hamline Open Access, accessed November 18, 2025, https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1261&context=mhlr
51. Van Loon - United States Court of Appeals for the Fifth Circuit, accessed November 18, 2025, https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf

52. Machine Learning | The University of Chicago Law Review, accessed November 18, 2025, https://lawreview.uchicago.edu/topic/machine-learning
53. Suspicious Activity Reports (SARs): A Compliance Guide - InnReg, accessed November 18, 2025, https://www.innreg.com/blog/suspicious-activity-reports-guide
54. A Guide to Fraud Protection with Suspicious Activity Reports - Flagright, accessed November 18, 2025, https://www.flagright.com/post/protecting-fintechs-and-neobanks-from-fraud-a
55. National Consumer Law Center RIN 3064-AF34 | FDIC, accessed November 18, 2025, https://www.fdic.gov/federal-register-publications/national-consumer-law-center
56. What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights - Frontiers, accessed November 18, 2025, https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.0003
57. What Is Predictive Policing and How Does It Impact Justice? - American Military University, accessed November 18, 2025, https://www.amu.apus.edu/area-of-study/criminal-justice/resources/what-is-pred
58. The Criminal Law and Law Enforcement Implications of Big Data - PMC - PubMed Central, accessed November 18, 2025,