The Epistemic Black Hole: Why the Deletion of Ballot Images Violates the Foundational Chain of Custody in Regulated Engineering Systems

A Quality Control and Data Provenance Framework for Optical Tabulation Systems

V.A. Shiva Ayyadurai, PhD. (M.I.T.)[1]

[1]International Center for Integrative Systems, 701 Concord Avenue, Cambridge, MA 02138.

Preprint Repository Version • Peer-Review Manuscript Track: Applied Case Studies & Quality Governance

Dedicated to my late father, V. Ayyadurai—a chemical engineer and master quality engineer who won multiple FDA awards for excellence in quality assurance. He introduced me to the rigorous discipline of quality engineering when I was twelve years old, as we worked together on engineering manuscripts during his tenure at Mennen and Colgate-Palmolive, following his earlier work at Shell and Parke-Davis. His uncompromising commitment to scientific integrity remains the foundation of this work.

ABSTRACT

In safety-critical, regulated engineering disciplines, the deterministic transformation of an analog physical artifact into an actionable tabular classification relies on unbroken data provenance. When an optical sensor ingests a physical object to generate an automated determination, foundational quality control (QC) frameworks—such as ISO/IEC 17025, GAMP 5, and AS9100—dictate that every intermediate representation in the computational chain must be immutably preserved. Purging intermediate image rasters severs the causal link between sensor input and algorithmic output, rendering downstream tabular metrics mathematically unverifiable. This paper demonstrates that the deletion or discretionary retention of ballot images violates the foundational chain-of-custody principles established across mission-critical systems engineering. We examine three benchmark industrial domains—aerospace computed radiography and optical inspection, pharmaceutical fill-finish parenteral inspection, and forensic 3D ballistic profilometry—detailing their end-to-end chain-of-custody protocols, the specific federal statutes and international quality standards they satisfy, and the catastrophic legal and operational consequences that occur when raw sensor records are discarded. We contrast these rigorous architectures with optical-scan election tabulation, where disparate state-level practices have historically treated digital ballot images as optional, ephemeral cache. Finally, we analyze the systemic auditability risks of image destruction under federal preservation law (52 U.S.C. § 20701), demonstrate how overlapping jurisdictional evasions create a closed loop of administrative unaccountability, and establish a mandatory engineering specification that eliminates administrative retention toggles in favor of cryptographically bound, dual-layer verification.

Keywords: Data Provenance, Chain of Custody, Quality Control, Optical Mark Recognition, Regulatory Asymmetry, ALCOA+, Measurement Systems Analysis (MSA), 52 U.S.C. § 20701.

1. Introduction: The Lineage Imperative in Measurement Systems

Measurement Systems Analysis (MSA) and quality assurance engineering proceed from an axiomatic baseline: an automated determination is only as reliable as its auditable data lineage [1]. In modern quality engineering, the transformation of physical inputs into digital classifications is modeled as a discrete state machine:

$$S_0 \xrightarrow{\mathscr{T}_{\text{sensor}}} S_1 \xrightarrow{\mathscr{A}_{\text{algorithm}}} S_2 \xrightarrow{\Sigma} S_3$$

Where S_0 is the physical, analog artifact under evaluation (e.g., an airframe weld, a drug vial, a cartridge casing, or a voter-marked paper ballot); $\mathscr{T}_{\text{sensor}}$ is the optoelectronic transfer function converting analog physical characteristics into digital sensor raw data; S_1 is the raw digital representation (e.g., a 16-bit radiograph, a 3D elevation mesh, or a 300 DPI duplex raster scan); $\mathscr{A}_{\text{algorithm}}$ is the deterministic classification or mark-sense algorithm evaluating spatial, volumetric, or densitometric features against predetermined control thresholds; S_2 is the tabular telemetry or record of decisions (e.g., void ratio, particulate count, striation correlation score, or Cast Vote Record [CVR]); and S_3 is the final aggregated state (e.g., batch release status, airworthiness certificate, criminal indictment, or certified election canvass).

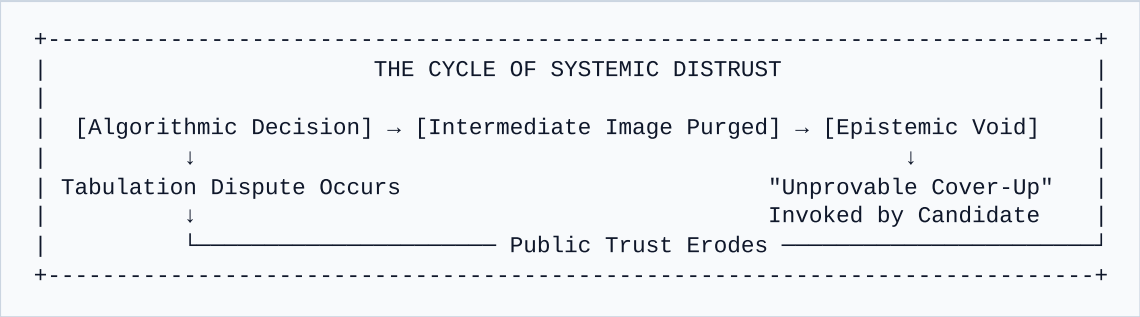
Under the universally accepted **ALCOA+** quality framework (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available) [9], an audit cannot validate the transition from S_0 to S_2 if the intermediate state S_1 is discarded. The microprocessor executing $\mathscr{A}_{\text{algorithm}}$ never interacts directly with S_0; it computes outputs *exclusively* from S_1.

Consequently, discarding S_1 creates an epistemic and operational discontinuity. In the presence of a discrepancy between S_0 and S_2, an auditor cannot determine whether the divergence stems from sensor noise, optical distortion, parameter drift, software bugs, or downstream physical alteration of S_0. Across regulated industry, treating S_1 as an ephemeral buffer rather than an archival record is considered a critical non-conformance.

2. The Epistemic Dilemma: An Unfalsifiable Claim

> **The Fundamental Dilemma of Image Deletion**
>
> *"I won the election, and the truth is you cannot disprove me."*

In public discourse surrounding contested elections, challenges to machine tallies are routinely characterized in political commentary as bad-faith opportunism. However, from a formal systems engineering and evidentiary perspective, when an optical-scan tabulator discards the digital image (S_1) that generated the tabular record (S_2), the challenger's assertion becomes **technically and mathematically unfalsifiable**.



When S_1 is erased, the state is forced to defend an abstraction (S_3) using only downstream summaries (S_2) and the upstream physical paper (S_0), while the actual computational object evaluated by the system has been destroyed. This creates two insoluble failure modes during disputes:

1. The Fraud Inversion Dilemma: If a post-election hand recount of physical paper ballots matches the electronic CVR tally, an adversarial challenger can allege that counterfeit physical ballots were introduced into storage boxes post-tabulation to match a corrupt machine tally. Without the timestamped, cryptographically hashed image captured at the moment of scanning, the state cannot prove that the paper in the box matches what the scanner observed on Election Day.

2. The Discrepancy Attribution Dilemma: If the physical paper recount diverges from the machine tally, administrators cannot demonstrate whether the scanner experienced an optomechanical misread or whether the physical ballots were degraded, lost, or manipulated while in physical transit and storage.

By deleting the intermediate image, the system forfeits its primary forensic defense. The challenger's claim cannot be mathematically disproven through algorithmic telemetry, converting what should be an objective engineering verification into an irreconcilable conflict of belief.

3. Industrial Benchmarks: The Three-Sector Gold Standard

In mission-critical, regulated industries, data provenance requires that raw sensor captures be treated as permanent evidentiary assets. The table below illustrates the profound regulatory asymmetry between established industrial mandates and electoral tabulation practices.

Industry Sector	Governing Standard / Law	Primary Sensor Object	Intermediate State	Consequence of Purging
Aerospace NDT & SMT Assembly	AS9100D [10] 14 CFR Part 21/43 [4] 18 U.S.C. § 38 [11]	Turbine Blade / Avionics PCBA Assembly	16-bit DICONDE / Raw CT Slices [2]	Grounding (EAD), Part Revocation, Prison.
Biopharmaceutical Manufacturing	21 CFR Part 11 [5] 21 CFR § 211.68 [6] FD&C Act [20]	Parenteral Drug Vial / HPLC Run	High-Speed Line Scan / Peak Files [16]	Form 483, Consent Decree, Plant Shutdown.

Industry Sector	Governing Standard / Law	Primary Sensor Object	Intermediate State	Consequence of Purging
Forensic Ballistics	ISO/IEC 17025 [8] FRE 702/901 [19] *Brady v. MD* [18]	Fired Cartridge / Toolmark	3D Confocal Microscopic Point Cloud [7]	Evidence Suppressed, Convictions Vacated.
Optical Election Tabulation	52 U.S.C. § 20701 [12] 52 U.S.C. § 20702 [13]	Voter-Marked Paper Ballot	Duplex 300 DPI Contact Image Sensor Scan	**Epistemic Black Hole, Systemic Distrust.**

3.1 Aerospace Manufacturing: Non-Destructive Testing (NDT) & SMT Inspection

Under AS9100D and Federal Aviation Administration (FAA) oversight, safety-critical aerospace components—such as rotating single-crystal turbine blades and flight-control Surface-Mount Technology (SMT) assemblies—undergo automated Non-Destructive Testing (NDT) via computed radiography, computed tomography (CT), and automated optical inspection (AOI).

Protocol & Custody Chain: Every blade carries a permanent, laser-etched 2D Data Matrix code compliant with MIL-STD-130. Before scanning, detector arrays are calibrated against NIST-traceable tungsten wire-pair image quality indicators (ASTM E1742 [3]). The raw 16-bit DICONDE image frames are streamed directly to Write-Once-Read-Many (WORM) storage, cryptographically hashed via SHA-512, and locked to the component serial number before algorithmic flaw-detection executes.

Consequences of Violation: Retaining a tabular "Pass" record while discarding the raw radiograph is a catastrophic non-conformance. Under 14 CFR Part 21 [4], components lacking primary inspection data are legally classified as Suspected Unapproved Parts (SUP), resulting in immediate Emergency Airworthiness Directives (EADs) that ground entire aircraft fleets. Under 18 U.S.C. § 38 [11], knowingly concealing or failing to maintain required inspection records carries federal criminal penalties of up to 15 years in prison.

The "Option" Absurdity: No aerospace software vendor would ever include a toggle allowing an operator to *"Discard CT Scans to Save Hard Drive Space."* The presence of such a feature would void FAA Part 145 repair station certification immediately.

3.2 Pharmaceutical Fill-Finish: Parenteral Inspection

Under current Good Manufacturing Practice (CGMP), injectable parenterals (vaccines, biologics) must undergo 100% automated visual inspection to detect container closure defects and sub-visible particulate matter per USP ⟨788⟩ [16] and ⟨790⟩ [17].

Protocol & Custody Chain: Vials rotate along a starwheel at up to 600 units per minute, spin at 3,000 RPM, and brake abruptly while high-speed line-scan cameras capture sequential backlit frames of the fluid meniscus. Prior to each run, the system must validate detection thresholds against certified challenge sets. Automated inspection machines commit all challenge-set frames and batch rejection sequences to validated Laboratory Information Management Systems (LIMS), signed with PKI-based electronic signatures and synchronized to UTC.

Consequences of Violation: Discarding raw high-speed frames or challenge runs while logging a "Lot Passed" determination violates 21 CFR § 211.194 [6]. The drug product is legally deemed *adulterated*. Violations result in FDA Form 483 inspectional observations, Warning Letters, and Department of Justice Consent Decrees of Permanent Injunction. Under the legal doctrine established in *United States v. Park* [20], corporate executives face strict criminal prosecutions for distributing adulterated product, regardless of personal knowledge or intent.

The "Option" Absurdity: In pharmaceutical software validation (GAMP 5) [9], treating raw sensor capture retention as an optional administrative preference is an automatic disqualifier. A system designed to delete primary sensor data is considered structurally defective.

3.3 Forensic Ballistics: 3D Surface Topography (NIBIN / IBIS)

The National Integrated Ballistic Information Network (NIBIN) digitizes the microscopic toolmarks left by firearms on spent cartridge casings recovered from crime scenes.

Protocol & Custody Chain: Confocal 3D profilers, calibrated with NIST-certified depth standards (±0.1 µm), capture the microscopic surface topology of the primer, breech face, and ejector marks, generating a 3D digital elevation model (DEM). The raw mesh is hashed via SHA-256 and stored in compliance with FBI CJIS standards [7] before correlation software calculates match probabilities.

Consequences of Violation: Presenting an algorithmic correlation score in court while failing to retain the underlying 3D topography violates Federal Rule of Evidence 702 and the *Daubert* standard [19], rendering the match inadmissible as unauthenticated hearsay. Under *Brady v. Maryland* [18], suppressing or destroying technical files that could impeach the algorithm constitutes a constitutional violation. In historical forensic lab scandals, the destruction of underlying analytical spectra resulted in the dismissal of over 20,000 criminal convictions.

The "Option" Absurdity: A forensic technician cannot argue: *"Our instrument detected a match, but our software discarded the 3D scan to conserve server storage."* The testimony would be stricken immediately and the examiner referred for spoliation sanctions.

4. The Electoral Anomaly: Ephemeral vs. Persistent States

In optical-scan election systems, paper ballots (S_0) pass through a feed path where contact image sensors (CIS) capture a duplex scan (S_1). Software then runs Optical Mark Recognition (OMR) algorithms to tabulate votes into a Cast Vote Record (S_2):



As confirmed explicitly by the state-issued vendor certification documents for the ES&S and Dominion tabulators used in benchmark jurisdictions [21]–[23]: **“Both sides of the ballot are processed simultaneously with high-resolution scanners and the resulting ballot images are decoded by a proprietary recognition engine”** [21], [22].

From a systems-engineering perspective, the digital image is not an optional afterthought; it is an indispensable intermediate computational artifact. The scanner hardware physically captures the image and generates a high-resolution electronic matrix in active memory. The software engine is mathematically blind without it. Consequently, a software toggle configured by an administrator to "disable" storage does not prevent the creation of the record; rather, it executes an **active software command to intercept and auto-delete a live federal data trail** before it can be committed to permanent storage.

```
                        CURRENT FLAWED ARCHITECTURE
[Paper Ballot] → [CIS Sensor] → [RAM Buffer] → [OMR Algorithm] → [Cast Vote Record]
                                      |
                                      └→ (Toggle: Save Image?) → NO  → (Purged)
                                                               → YES → (Retained)

                   REQUISITE HIGH-ASSURANCE ARCHITECTURE
[Paper Ballot] → [CIS Sensor] → [WORM Storage + SHA-256] → [OMR Algorithm] → [Cast Vote Record]
                                      |                                          |
                                      └──────────────────(Cryptographic Binding)─┘
```

Despite the strict mathematical dependence of the Cast Vote Record on the digital raster image:

- Legacy tabulator architectures were engineered with administrative toggles permitting operators to disable image saving or overwrite memory media post-canvass.
- Several state election divisions historically interpreted “record retention” as applying strictly to physical paper, treating the digital image as an ephemeral processing artifact.
- In high-reliability engineering, executing an automated transformation while deliberately discarding the input is an architectural anti-pattern that violates basic principles of measurement validation.

5. Statutory Harmonization and the Fallacy of Administrative Discretion

This jurisdictional and engineering conflict is not merely theoretical; it is currently the subject of active litigation. Recent federal and state mandamus proceedings (e.g., *Ayyadurai v. Galvin et al.*, 2026) [15] provide an applied case study of this tension, wherein state election officials invoke domestic equipment certification rules to justify the deliberate disabling of digital image storage. However, the claim that local election jurisdictions possess the legal discretion to purge digital ballot images contradicts federal statutory law on two primary fronts.

5.1 The Supremacy Clause and the Federal Mandate Under Title III

Title III of the Civil Rights Act of 1960 (52 U.S.C. § 20701 [12]) establishes an unambiguous statutory baseline:

> *"Every officer of election shall retain and preserve... for a period of twenty-two months from the date of any general, special, or primary election... all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election..."*

Furthermore, 52 U.S.C. § 20702 imposes criminal penalties on any custodian who willfully steals, destroys, conceals, mutilates, or alters any record covered by Section 20701 [13].

A state official cannot utilize domestic equipment approval laws to systematically bypass an explicit federal criminal mandate. Under the **Supremacy Clause (Art. VI, cl. 2)** and the **Elections Clause (Art. I, § 4, cl. 1)**, when Congress occupies the field regarding the preservation of federal election data, its enactments completely preempt conflicting state administrative rules. As the United States Supreme Court held in *Arizona v. Inter Tribal Council of Ariz., Inc., 570 U.S. 1, 9 (2013)* [24], "The Elections Clause empowers Congress to pre-empt state regulations governing the Times, Places and Manner of holding Congressional elections... State regulations in this area remain legal only so long as they do not conflict with an act of Congress."

5.2 The Technical Fallacy of “Paper-Only” Exemptions

Administrative attempts to exempt ballot images from Section 20701 fail on two grounds:

- **The Computational Act Requisite to Voting:** In an optical tabulator, the physical paper never interacts with the microprocessor. The optical sensors convert the paper into a raster image, and the software tabulates votes *exclusively* from that digital file. The image is an indispensable “act requisite to voting”—without it, no tabulation occurs.
- **Dual-Record Custody:** The Civil Rights Division of the Department of Justice has repeatedly affirmed that Section 20701 applies to electronic records, including digital ballot images, CVRs, and audit logs [14]. Furthermore, **the physical paper ballot and the corresponding digital image generated by the scanner in active memory are separate, concurrent records under federal law.** Both exist, both are part of the electronic chain of custody, and both are subject to the 22-month federal retention requirement.

5.3 The Jurisdictional Accountability Vacuum

The applied case study of *Ayyadurai v. Galvin et al.* [15] exposes a critical flaw not just in tabulation architecture, but in the corresponding legal architecture intended to regulate it. When a candidate seeks enforcement of 52 U.S.C. § 20701, a closed-loop jurisdictional evasion often emerges:

- State courts assert that because Congress did not construct an explicit private right of action for individual candidates under § 20701, enforcement power is reserved exclusively for the Department of Justice (DOJ).
- The DOJ, despite publishing formal advisories recognizing ballot images as protected federal records, frequently remains silent and abstains from initiating enforcement actions.
- When federal enforcement is subsequently sought in a U.S. District Court under the Supremacy Clause, the federal judiciary invokes procedural doctrines (such as *Rooker-Feldman* and *Colorado River* abstention) to decline jurisdiction, citing deference to the very state court proceedings that deferred to the federal government.

The result is a Kafkaesque accountability vacuum. The state claims it is simply following its own domestic rules; the state judiciary points to the DOJ; the DOJ does not act; and the federal judiciary points back to the state court. In this loop, no single node takes responsibility for evaluating the foundational engineering reality: the microprocessor tabulates the digital image in RAM, not the physical paper ballot in the bin. This legal runaround perfectly mirrors the broken chain of custody in the tabulation hardware itself.

6. High-Assurance Architectural Specifications

To align election systems with industrial engineering and data integrity benchmarks, all voting tabulators must enforce the following foundational architectural specifications to guarantee end-to-end chain of custody:

6.1 Hardware-Enforced Non-Volatile Commits

In legacy architectures, image retention was frequently governed by software toggles managed by the Operating System, allowing field operators to disable the save function. A high-assurance architecture requires that the commitment of the image file to storage be enforced at the hardware or firmware level. Systems must utilize Write-Once-Read-Many (WORM) storage controllers that physically prohibit memory allocation from clearing an image raster out of volatile RAM until the duplex scan is successfully written to the non-volatile disk. The administrative option to bypass or disable image saving must be permanently removed from the firmware logic.

6.2 Deterministic Cryptographic Binding

A persistent vulnerability in basic database architecture is the creation of "orphan records"—where an image file exists without a corresponding database row, or a vote tally exists without a source image. To satisfy ALCOA+ standards for complete data lineage, the system must execute deterministic cryptographic binding. Upon ingestion, the tabulator must calculate a SHA-256 hash of the image file. This hash, alongside the physical batch identifier (e.g., scanner ID and bin number) and the digital image's Unique Identifier (UID), must be inextricably appended as a primary key to the Cast Vote Record (CVR) row. This prevents bad actors from laterally modifying a text-based CVR without immediately invalidating the cryptographic relationship to the immutable image.

6.3 The Privacy Fallacy and Cryptographic Permutation

Administrative bodies frequently invoke voter privacy—specifically the risk that sequential timestamps could theoretically map a specific voter to a specific ballot image—as a justification for purging digital records. In modern systems engineering, this is a false dichotomy and a structurally solved problem. **Destroying primary sensor data to protect privacy is akin to a hospital incinerating medical records rather than encrypting them.**

To resolve this without destroying the evidentiary trail, engineering systems must simply employ privacy-preserving cryptographic permutations (shuffling). Rather than recording the exact sequential millisecond of ingestion in the public metadata, the system can batch images and apply a cryptographic salt to randomize their storage order. This decisively breaks the sequential link between voter check-in and ballot processing, completely preserving the secret ballot while maintaining the mathematical integrity and auditability of the aggregate count.

6.4 Open Public Image Repositories

Consistent with modern transparency practices in open-source software and public-sector quality assurance, the resulting cryptographic image archives must not be treated as proprietary black-box data. Upon certification of the canvass, these archives should be made fully accessible to the public domain. This enables crowdsourced quality assurance, allowing academic institutions, independent auditors, and public citizens to run third-party Optical Mark Recognition (OMR) software against the public images, independently verifying the state's arithmetic and restoring mathematically proven public confidence.

7. The Parable of the Weighmaster’s Camera

To distill the sociotechnical and epistemic consequences of purging intermediate sensor data, we present a brief narrative allegory. This parable translates the cryptographic and systems-engineering vulnerabilities detailed above into a fundamental illustration of human trust, demonstrating why the preservation of intermediate measurement states is the bedrock of verifiable science.

> **THE PARABLE OF THE WEIGHMASTER’S CAMERA**
>
> In an ancient market town, grain was sold not by standard weights, but by a machine built by an ingenious guild. A farmer would pour his sack of grain into an iron hopper, and an optical apparatus —a dark box containing mirrors and photosensitive paper—would capture the silhouette of the falling grain against a grid of light.
>
> Inside the box, mechanical levers read the silhouette, calculated the density and volume of the shadows, and stamped a brass token: "This sack equals 500 pounds of grain."
>
> For years, the merchants and farmers trusted the brass tokens. But as rivalries grew fierce and the price of grain skyrocketed, a merchant brought fifty prized sacks of wheat to the hopper. The machine clattered, the levers clicked, and the tokens dropped: "400 pounds per sack."

> The merchant was furious. "My fields have never yielded less than 500 pounds a sack!" he yelled. "Your machine has cheated me! Show me the proof!"
>
> The Chief Weighmaster smiled calmly and led the merchant to the back room. "Do not fret," the Weighmaster said, pointing to fifty woven sacks stacked in the storeroom. "We have the grain right here. We can pour it into buckets and weigh it by hand with iron stones."
>
> "I don't care about the sacks sitting in your open room!" cried the merchant. "Anyone could have scooped out wheat while you carried them in here, or swapped my sacks for inferior grain! Show me the picture the machine took when I poured it! Show me the silhouette that your levers measured!"
>
> The Weighmaster blinked. "Ah. Well, to save room in our filing cabinets, we immediately burn the photograph the second the brass token drops. We only keep the token and the grain."
>
> The merchant stood in the town square and addressed the crowd: "The Weighmaster stole my harvest! And the proof that he stole it is that he burned the very picture his machine used to calculate my ruin! I tell you I brought 500 pounds, and the truth is, you can never disprove me!"
>
> The Weighmaster called thirty respected elders to weigh the grain by hand with iron stones. The stones read 400 pounds. The Weighmaster declared himself vindicated.
>
> Yet half the town walked away unconvinced. For they realized that while the grain on the floor might indeed weigh 400 pounds, the Weighmaster could never prove what fell through the hopper that morning. By burning the photograph, the Weighmaster had made the machine's inner mind invisible. He had given the merchant a permanent, unanswerable argument—and reduced a brilliant science back into a matter of mere belief.

8. Conclusions and Discussion

The integrity of an automated measurement system relies absolutely on the preservation of its primary sensor data. Through the lens of industrial quality control and systems engineering, optical-scan election tabulators are not merely counting mechanisms; they are complex optoelectronic sensors. The microprocessor executing the tabulation logic does not evaluate the physical paper ballot; it evaluates the digital image raster generated by the Contact Image Sensor (CIS). Consequently, the digital ballot image is the indispensable intermediate state—the direct causal parent of the Cast Vote Record.

As demonstrated across the aerospace, pharmaceutical, and forensic science sectors, the destruction of intermediate sensor states is universally recognized as a catastrophic breach of quality assurance. This disparity reveals a profound regulatory asymmetry: the administrative state imposes strict liability, institutional shutdowns, and federal prison sentences on engineers in the private sector for failing to preserve raw intermediate sensor data, while simultaneously procuring and deploying public voting architectures that are expressly configured to intercept and purge that exact same class of data. This discrepancy is not merely a software glitch or an administrative oversight; it is an architectural anti-pattern designed to enforce absolute systemic unaccountability.

Furthermore, state-level administrative practices that permit the deletion of these images stand in direct conflict with the federal retention mandates of 52 U.S.C. § 20701. To restore epistemic trust and align democratic infrastructure with the universal ALCOA+ principles of systems engineering, election technology must evolve. By mandating hardware-enforced image retention, cryptographic binding, and open-source public verification, election administrators can close the epistemic black hole, decisively neutralizing unfalsifiable claims of fraud and ensuring that election outcomes are rooted in verifiable, transparent data science.

9. References

1. **American Society for Quality (ASQ).** (2020). *Measurement Systems Analysis (MSA) Reference Manual*, 4th Edition. Automotive Industry Action Group (AIAG) / ASQ.
2. **ASTM International.** (2018). *ASTM E2339-15: Standard Practice for Digital Imaging and Communication in Nondestructive Evaluation (DICONDE)*. West Conshohocken, PA.
3. **ASTM International.** (2021). *ASTM E1742/E1742M-18: Standard Practice for Radiographic Examination*. West Conshohocken, PA.
4. **Code of Federal Regulations.** (2024). *Title 14, Part 21: Certification Procedures for Products and Articles*. Federal Aviation Administration, Department of Transportation.
5. **Code of Federal Regulations.** (2024). *Title 21, Part 11: Electronic Records; Electronic Signatures*. Food and Drug Administration, Department of Health and Human Services.
6. **Code of Federal Regulations.** (2024). *Title 21, Part 211: Current Good Manufacturing Practice for Finished Pharmaceuticals*. Food and Drug Administration.
7. **Federal Bureau of Investigation (FBI).** (2022). *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.9. U.S. Department of Justice.
8. **International Organization for Standardization.** (2017). *ISO/IEC 17025:2017: General requirements for the competence of testing and calibration laboratories*. Geneva, Switzerland.
9. **ISPE.** (2008). *GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems*. International Society for Pharmaceutical Engineering (ISPE).
10. **SAE International.** (2016). *AS9100D: Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations*. Warrendale, PA.
11. **United States Code.** *Title 18, Section 38: Fraud involving aircraft or space vehicle parts in interstate or foreign commerce.*
12. **United States Code.** *Title 52, Section 20701: Retention and preservation of records and papers by officers of elections; deposit with custodian; penalty for violation.*
13. **United States Code.** *Title 52, Section 20702: Theft, destruction, concealment, mutilation, or alteration of records or papers; penalties.*
14. **U.S. Department of Justice.** (2021). *Federal Law Obligations Regarding Post-Election Audits and Retention of Election Records*. Civil Rights Division, Washington, D.C.
15. **U.S. Court of Appeals for the First Circuit.** (2026). *Ayyadurai v. Galvin et al.*, Interlocutory Appeal per 28 U.S.C. § 1292(a)(1).
16. **U.S. Pharmacopeia (USP).** (2023). *General Chapter ⟨788⟩: Particulate Matter in Injections*. Rockville, MD.
17. **U.S. Pharmacopeia (USP).** (2023). *General Chapter ⟨790⟩: Visible Particulates in Injections*. Rockville, MD.
18. **Supreme Court of the United States.** *Brady v. Maryland*, 373 U.S. 83 (1963).
19. **Supreme Court of the United States.** *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

20. **Supreme Court of the United States.** *United States v. Park*, 421 U.S. 658 (1975).
21. **Office of the Secretary of the Commonwealth of Massachusetts.** (2014). *Approval of Voting Equipment in Massachusetts: ES&S DS200 Precinct Tabulator (EVS 5.0.0.3)*. Elections Division.
22. **Office of the Secretary of the Commonwealth of Massachusetts.** (2020). *Approval of Voting Equipment in Massachusetts: ES&S DS450 Central Tabulator (EVS 5.3.4.0)*. Elections Division.
23. **Office of the Secretary of the Commonwealth of Massachusetts.** (2014). *Approval of Voting Equipment in Massachusetts: Dominion ImageCast Precinct Tabulator (ICP)*. Elections Division.
24. **Supreme Court of the United States.** *Arizona v. Inter Tribal Council of Ariz., Inc.*, 570 U.S. 1 (2013).



Dr. V.A. Shiva Ayyadurai is a world-renowned systems scientist, inventor, and entrepreneur who holds four degrees from the Massachusetts Institute of Technology (MIT), including a B.S. in Electrical Engineering and Computer Science, a dual Master's in Mechanical Engineering and Visual Studies from the MIT Media Laboratory, and a Ph.D. in Systems Biology from the Department of Biological Engineering.

Recognized as the inventor of email, Dr. Ayyadurai developed the first electronic emulation of the entire interoffice mail system in 1978 at the age of 14, for which he was awarded the first United States Copyright for "Computer Program for Electronic Mail System." His pioneering research on pattern recognition, large-scale systems development, and computational biology has resulted in numerous commercial products, patents, and publications in leading scientific and engineering journals, including *Nature*, *CELL*, and *IEEE*.

He is the Chairman & CEO of CytoSolve, Inc., providing a computational platform for modeling complex diseases. Beyond his scientific and entrepreneurial achievements, Dr. Ayyadurai is an active civic leader who has run as a candidate for the United States Senate in Massachusetts and for President of the United States. He is a Fulbright Scholar, a Westinghouse Science Talent Honors Award recipient, and a Lemelson-MIT Awards Finalist.