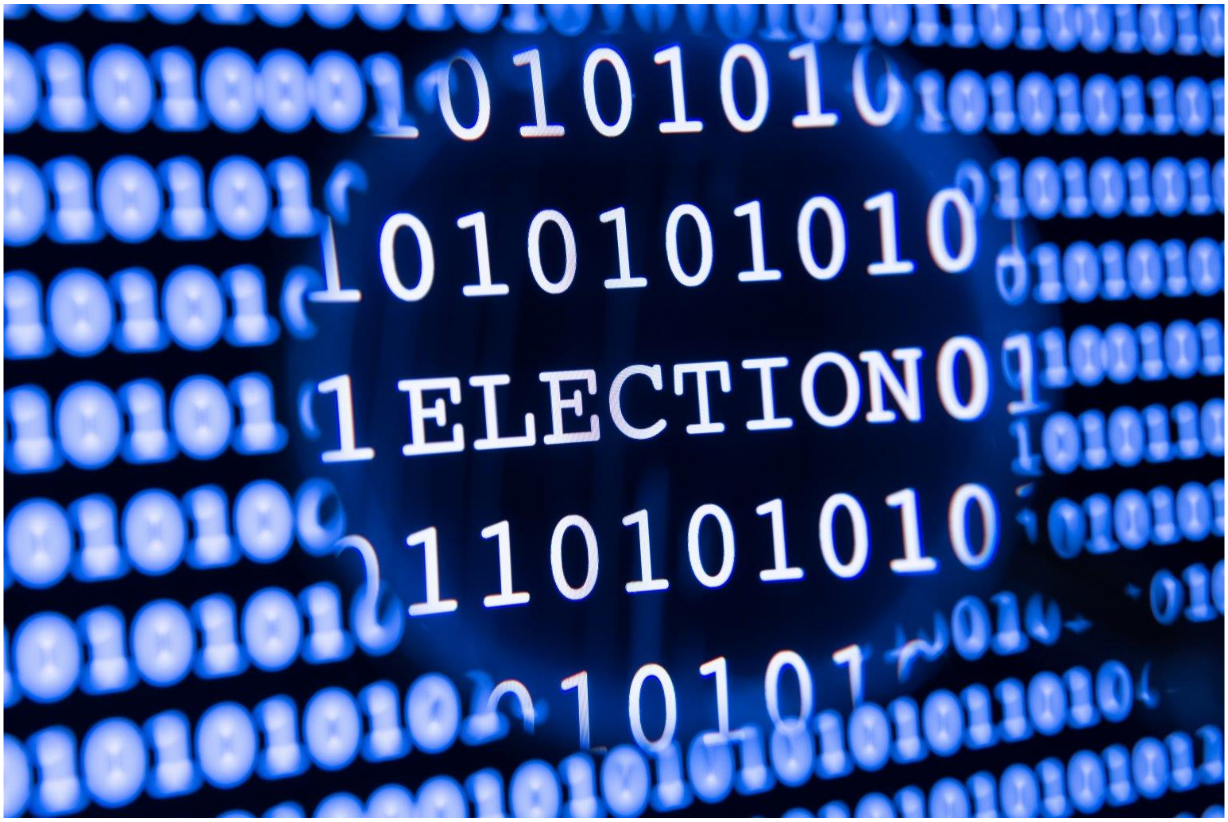
Hidden Infrastructure of Voter Surveillance:

Potential Evidence of an Unlawful Relational Database Linking Ballots to Voters



ELECTION FAIRNESS INSTITUTE

An EFI White Paper – For Public Release

Hidden Infrastructure of Voter Surveillance:

Potential Evidence of an Unlawful Relational Database Linking Ballots to Voters

By: A. Campbell/TBTR Strategies

Executive Summary

This report details extensive findings suggesting the unlawful construction and use of a relational database that can track ballots back to individual voters, thereby violating federal and state protections of ballot secrecy. We draw on public records, grassroots investigations, and expert analyses to identify troubling patterns. Contributors include Barry Wernick, Dr. Andrew Paquette, Susan Valiant, TBTR Strategies, Dr. Laura Pressley, and others. Together, their findings outline a system design and series of activities that undermine the very integrity and transparency of elections. This pattern is evident in multiple jurisdictions, including Tarrant County and Dallas County in Texas, Nassau County in New York, and potentially in every county that relies on computerized voting systems.

I. Introduction

The secrecy of the ballot is a bedrock principle of democratic elections, mandated by both Texas and federal law. However, research conducted by multiple independent teams, compiled by TBTR Strategies, reveals an alarming pattern in which computerized voting systems—especially those employing electronic poll books (e-poll books), ballot marking devices (BMDs), and integrated ballot printers—are producing ballots embedded with identifiable data linked directly to voter check-ins. These identifiers may take the form of barcodes, QR codes, access codes, or hexadecimal-style numerical tags.

Through both human-readable and machine-readable formats, voter data from check-in to ballot creation is potentially being used to build covert and unlawful relational databases, permitting administrative actors or external entities with administrative access, to associate individual ballots with specific voters, in direct violation of constitutional and statutory mandates. Independent researchers report the potentially unlawful inflation and deflation of active voter rosters both pre and post-election, inconsistent vote totals between county and state reports, the facilitation and obfuscation of the replacement of electronic totals and physical ballots, and the inability to audit records to detect these issues inherent in modern computerized voting systems.

II. Technical Breakdown: How Voter Data is Embedded into Ballots

A. The Role of E-Poll Books and Ballot Printers

In Dallas County, ES&S e-poll books were discovered to have glitched during a recent general election, failing to complete voter check-ins and printing ballots with repetitive barcodes used to create the "ballot style" for the voter. This malfunction in the ES&S e-poll book equipment resulted in an untold number of voters receiving the wrong ballot style— meaning multiple voters received the same ballot tied to a single incomplete check-in.

These ballot identifiers, printed from e-poll books directly, or using a peripheral machine to transcribe e-poll book barcodes created for each voter, included human-readable and machine-readable codes (barcodes or hexadecimal-like identifiers) that were transferred from the e-poll book to the ballot marking device, and then on to the ballot which is then scanned into a thumb drive. In many cases it is known that these incorrect ballots were printed and then unknowingly voted and cast, without these voters even being formally checked in, as the e-poll books were stuck on the initial voter scanned in, and kept printing ballots for that original voter only, without anyone noticing. Election judges had no idea the voters they were scanning were not being checked in, and that they were all getting the same ballot style. This lack of understanding of how to conduct computerized elections and detect serious issues has created opportunities for multiple votes to be cast by or on behalf of a single registration without detection.

These system malfunctions were later patched mid-election through a firmware update, raising serious concerns about the legal chain of custody, the auditability of ballots, and the security of the voting process.

B. QR Codes and Access Codes as Data Carriers

In systems like HART InterCivic's Verity Voting, a barcode generated at check-in is translated via a peripheral controller, typically into a six-digit access code that must be manually entered by the voter into the ballot-marking device to create that voter's unique ballot. After voter selections are made, a QR code, and often an additional mysterious number, which has gone unexplained by even this author's friend, Heider Garcia, is printed onto the ballot along with the voter selections. The structure of this data pathway suggests a multi-step digital fingerprinting process by which a single code, tied to the voter's check-in, survives through every step of the voting process—from check-in to ballot generation to casting and potentially beyond.

Election officials claim that these codes contain no voter-identifiable information. However, without full transparency and vendor cooperation—and under threat of legal consequences for inspecting proprietary software—we cannot verify these assurances. The very structure of these systems, as demonstrated by technical audits and whistleblower reports, indicates the presence of relational logic: one piece of data triggering another, across multiple devices, creating a traceable chain.

III. Legislative and Procedural Failures

A. The SOS Redaction Order and its Implications

The Texas Secretary of State (SOS) issued a directive after the 2024 primary election requiring the redaction of “personally identifiable” information from cast ballot images and election records. This move followed reports—initiated by grassroots investigator and attorney Barry Wernick—revealing that ballots across multiple counties could be matched to individual voters using publicly available election data.

Rather than admit to a systemic issue, the SOS sought to cover it up through redactions, thus acknowledging the problem while simultaneously hiding its scale. This redaction policy placed local election officials in the position of determining what data was "personally identifiable," leading to inconsistent applications and further violations of transparency statutes.

This very act undermines the statutory mandate that all ballots must be anonymous at the time of creation and violates public access rights under both state and federal law.

IV. Ballot Fraud by Design: A Workflow for Undetectable Manipulation

The Election Fairness Institute, with the investigative services of TBTR Strategies, has compiled all the available evidence from our own research, and from thorough examination of work completed by other dedicated American Patriots, that when compiled logically, seem to document a full chain of election manipulation, using both technical and procedural vulnerabilities:

1. ***Inflation of Voter Rolls***: Pre-election increases in active voter registrations, including reactivation of inactive voters.
2. ***Ballot Generation Loopholes***: Unlimited ballots are potentially created under one check-in, with systems not designed, purposely or mistakenly, to flag duplicate ballots.
3. ***Non-Sequential Ballot Numbering***: Vendors have improperly advised counties to eliminate sequential numbering, making insertion of fraudulent ballots undetectable.
4. ***Excess Ballot Stock***: Thousands of additional blank ballots were allocated to polling locations with historically low turnout. TBTR Strategies trained poll watchers have observed that election judges were taught only to count ballot stock on the log forms as they opened a packet, leaving thousands potentially unaccounted for. We are only aware of these excessive ballot stock allocations because of properly trained poll watchers diligently reporting the divergences.
5. ***Ballot Swapping and Mishandling***: Election judges observed opening and sorting of cast ballots from ballot boxes after the close of polls, in violation of chain of custody.
6. ***Broken, Missing or Incomplete Chain of Custody***: The removal of lawful ballots and insertion of fraudulently created ballots could be occurring countywide with the severe

Chain of Custody violations documented by properly trained poll watchers. This is the only evidence the county and state has to prove that a lawful, trustworthy and accurate election was properly conducted. Without having reliable and properly trained poll watchers, these acts of impropriety will continue to occur without voter knowledge or for there to be a hope of intervention to correct this practice.

7. ***Vote Collapsing and Registration Removal***: Post-election, fake registrations are returned to inactive or suspended status, obscuring voter history and eliminating traces of any fake votes having been included, while county and state vote totals and voter turnout records fail to reconcile.

In short:

We believe that, prior to an election, inactive or suspended voters are somehow digitally reactivated. Polling places are then equipped with electronic poll books that track voter turnout across the county and assign some form of data to each ballot at check-in. These locations are often overstocked with ballots that are improperly tracked.

After the election, we suspect that fake (ghost) voters are then “removed” from the system and fraudulent ballots are created and inserted without detection, sometimes accompanied by unauthorized thumb drives containing data. Additionally, we believe that lawful ballots may be removed from ballot boxes after being counted and sorted. Ballots deemed “undesirable” could easily be swapped out before they are delivered to the central election office—either on election night or during the early voting period.

V. Data Pattern Analysis: The Findings of Dr. Andrew Paquette

Dr. Andrew Paquette’s research in Nassau County and across other jurisdictions provides critical technical validation of EFI’s findings. His forensic audits uncovered algorithmic patterns within voter registration files that indicate:

- Cloning of voter files through dual IDs linked to a hidden third.
- Predictable numerical patterns occurring every tenth entry—indicating algorithmic assignment.
- Removal of voters after elections, with corresponding changes in status from active to inactive or suspended.

These anomalies match the patterns uncovered by Susan Valiant, Barry Wernick, and others in multiple Texas counties, and add technical encumbrance to claims of a relational database underpinning the voter rolls, which we have already shown have data linked directly to the ballot from the e-poll books (voter rolls), what is supposed to be a separate database.

VI. The Legal and Constitutional Framework

The Texas Constitution demands that elections be conducted in a manner that preserves the purity of the ballot box, through ballot secrecy, auditability and strong election laws preventing undue influence and improper practice. The United States Constitution and federal law similarly require the protection of voter privacy, access to meaningful audits, and free and fair elections.

Every analysis outlined in this report—whether in the form of broken chain of custody, insertion of machine-generated identifiers, or unlawful redactions—represents a violation of these core principles. A system that inherently contains a secret database enabling the kind of activity we appear to have detected would be absolutely, 100% illegal and unlawful—if, in fact, that such a system does exist and has been used in U.S. elections. The subversive actions of such a criminal matter would introduce a calamity of crisis unexperienced in all of U.S. history.

VII. Conclusion

The convergence of technical malfunctions, unusual voter registration patterns, procedural irregularities, and embedded identifiers on ballots cannot be dismissed as mere coincidence or clerical error. Taken together, these findings form a cohesive body of evidence pointing to the likely existence of a relational database that unlawfully links ballots to individual voters—potentially enabling the tracking of fraudulent registrations for the purpose of collapsing them after the election.

This database not only facilitates the insertion and deletion of both ballots and voter records but also ensures that such manipulation remains undetectable without access to proprietary systems currently shielded by legal threats and vendor contracts. The database infrastructure is protected by a veneer of procedural legitimacy, but its function appears to be, potentially, entirely unlawful.

This phenomenon, by all properly administered analysis, can only occur at the administrative level. To investigate further, we will need full access to the entire election voting system for every State. Our goal is to determine whether additional evidence supports the existence of the relational database documented by Dr. Andrew Paquette, TBTR Strategies and the Election Fairness Institute. The work is supplemented by research from election subject matter experts such as Susan Valiant, Barry Wernick, Dr. Laura Pressley, and other unnamed volunteers who have devoted significant amounts of their time, energy, resources, and reputations to this cause. These efforts aim to help us all better understand how best to secure our elections against all undue influence and improper practices.