

From X user WalterZoom (@ZoomWalter) in this post:  
<https://x.com/ZoomWalter/status/1895869759381451106>

In a rush to support ballot secrecy (required by law), some are destroying auditability (also required by law) in certain cases. So when two laws conflict, which one do you follow? Here's my analysis:

### Auditability of Elections Trumps Ballot Secrecy

Two fundamental principles of fair and trustworthy elections are ballot secrecy and auditability. Ballot secrecy is tremendously important, to protect the voter against coercion, intimidation, blackmail, and the like, and also the temptation to sell one's vote. In 1948 vote buying in all its various forms became a federal crime (18 U.S.C. § 597). In Texas, Election Code § 122.001(a)(1) mandates that "A voting system may not be used in an election unless the system preserves the secrecy of the ballot."

Auditability is likewise tremendously important, since passing a complete forensic audit (not just a recount or a random sample or a risk-limiting audit) is the ultimate proof that the results of an election are accurate. Federal law 52 U.S.C. § 21081(a)(2) says:

(A) In general

The voting system shall produce a record with an audit capacity for such system.

(B) Manual audit capacity

(i) The voting system shall produce a permanent paper record with a manual audit capacity for such system.

(ii) The voting system shall provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced.

(iii) The paper record produced under subparagraph (A) shall be available as an official record for any recount conducted with respect to any election in which the system is used.

In Texas, Election Code § 122.001(a)(10) mandates that "A voting system may not be used in an election unless the system is capable of providing records from which the operation of the voting system may be audited."

Beginning with the Civil Rights Act of 1960 (and fair and honest elections are indeed our foundational civil right on which all other civil rights depend), section 301 explicitly required the preservation of all records relating to any "act requisite to voting"; this is now codified at 52 U.S.C. §§ 20701-20706. Note that per U.S. Department of Justice Publication "Federal Law Constraints on Post-Election 'Audits,'" July 28, 2021, the "materials covered by Section 301 extend beyond 'papers' to include other 'records.'" Jurisdictions must therefore also retain and preserve records created in digital or electronic form." This necessarily includes ballot images, computer hard drives, removable memory cards, surveillance video footage of ballot dropboxes, etc., in addition to physical ballots, outer envelopes and signatures on absentee ballots, and so on.

Following the principles enunciated in the July 28, 2021, DOJ publication just quoted, a searchable electronic form of the "permanent paper record with a manual audit capacity" (see 52 U.S.C. § 21081(a)(2) above) is also covered. Since this audit record must be permanent, that supersedes the 22-month retention period. Thus, electronic ballot images, Cast Vote Record ("CVR") reports, and so forth, may not ever be deleted unless, at a minimum, the required "permanent paper record with a manual audit capacity" has been created and maintained.

The primary tool for auditing elections is the report of each CVR, which is defined federally by the National Institute of Standards and Technology at <https://doi.org/10.6028/NIST.SP.1500-103> (“NIST”) as “an electronic record of a voter’s selections” and defined by the Texas Secretary of State as the “Permanent record of all votes produced by a single voter whether in electronic or paper copy form” (<https://sos.state.tx.us/elections/laws/electronic-voting-system-procedures.shtml>). In the case of an electronic record, NIST section 3.5.4 mandates that “For ballot-level comparison audits, there must be a means for pairing a CVR to its corresponding paper ballot.”

The NIST requirements were authorized by the 2002 Help America Vote Act, which directed NIST to promulgate standards for what must be included in a CVR. In addition to the voter’s selections and the means for pairing a CVR to its corresponding paper ballot, this includes, among other things, the BallotStyleID (which identifies the precinct, precinct split, etc.), and the BatchID and BatchSequenceID. These last two fields are crucial to auditing the sequence in which votes were tabulated, which recounts or random samples or risk-limiting audits do not check.

Since ballot secrecy and auditability are both required by law (cited above), ideally both ballot secrecy and auditability could be 100% satisfied in every election. However, there may be some situations where 100% ballot secrecy and 100% auditability conflict; that is, enforcing 100% ballot secrecy would prevent 100% auditability, or enforcing 100% auditability would prevent 100% ballot secrecy. In those cases, which is more important?

Note that it is common for laws to conflict, in which case a decision must be made as to which law takes precedence. For example, one law says to come to a complete stop at a stop sign, and another law says to obey law enforcement officers. So, what do you do when you approach a stop sign and a policeman waves you to proceed through the intersection without stopping? Obviously, you keep rolling, since the second law trumps the first. In cases where the priority is not clear, a court decision may be needed (see the Sewell decision below).

Similarly, careful consideration (detailed below) reveals that, if there is a conflict, auditability must trump ballot secrecy. After all, if the results cannot be proven to be accurate by a full forensic audit, then why bother to hold an election?

So how can such a conflict arise? In most modern voting systems, once the voter has been checked in, all connection to the voter is broken, and there is no personally-identifiable information on the ballot (no name, address, voter ID, etc.). This break is what enables the switch from secret voting to transparent public counting. As the South Carolina Constitution puts it, “All elections by the people shall be by secret ballot, but the ballots shall not be counted in secret.”

The overarching reason for transparency in counting is to ensure that the process is fair and honest, so that citizens can be confident that the election results are accurate and have not been tampered with. As the Texas Constitution says in Article 6, Section 4, “In all elections by the people, the vote shall be by ballot, and the Legislature shall provide for the numbering of tickets and make such other regulations as may be necessary to detect and punish fraud and preserve the purity of the ballot box; and the Legislature shall provide by law for the registration of all voters.”

This important transparency in counting is carried out by having more than one election officer doing the counting, as well as observers, including representatives of the opposing candidates on the ballot.

Having multiple eyes on the process thus helps “to detect and punish fraud and preserve the purity of the ballot box” from the defilement of inaccurate results.

Another vital aspect of transparent counting is the ability to completely audit an election. This is required by federal and state laws, as quoted above. Every CPA or financial officer knows what is necessary for a complete and verifiable audit—physical security, inventory, chain of custody, separation of duties, a complete audit trail, and so on. In everyday language, there must be sufficient data to reconstruct and trace all transactions, in effect to be able to make a “movie” after the fact of everything that happened before, during, and after an election.

This leads to a key example of why auditability trumps ballot secrecy. In a few rare instances, complete transparency including the BatchID and BatchSequenceID could lead to the identification of the voter who cast a particular ballot.

Example 1: Suppose you were second in line when the polling place opened and recognized the person ahead of you as your neighbor. Then when the official CVR is released you could look up the cast vote record for batch 1, batch sequence 1, and know how your neighbor voted. To protect against this, all electronic voting machine companies shuffle the records within each batch (of typically 100 ballots) to produce the CVR report. As a result, all you would know is that your neighbor’s ballot was one of the 100 ballots in batch 1; in other words, you would not know how they voted. This shuffling within each batch thus makes it possible to satisfy both the requirement of being auditable (namely, this batch of 100 voters cast these 100 ballots) with the requirement of ballot secrecy and voter privacy (namely, you cannot tell which voter cast which ballot).

Fortunately, shuffling the records within each batch does not destroy the ability to audit the sequence of batches for anomalies (like vote-stuffing) which cannot be detected by recounts or random samples or risk-limiting audits; it only makes the resulting graphs coarser without changing the shape of the graphs. Unfortunately, in a misguided attempt to address this rare example and other similar examples, some counties have illegally shuffled the entire CVR (as Maricopa County, Arizona, did in November 2022) or even deleted the BatchID entirely. Altering or concealing election data like this is a federal crime subject to serious penalties (52 U.S.C. § 20702).

It goes without saying that the county (or parish) has no obligation to protect a voter from revealing how they voted, for example by telling a reporter doing exit polls, or by signing an absentee ballot itself (violating the explicit instructions not to make any stray marks on the ballot and only sign the outside affidavit envelope, which is separated from the ballot when it is received by the county). This is the choice and responsibility of the voter to breach their own privacy.

Similarly, the county has no obligation to prevent the unavoidable loss of privacy when logical deduction can reveal how someone voted.

Example 2: Suppose there are 100 votes in a particular race between two candidates, A and B, and the count is 100 for A and 0 for B. Then you know each of the 100 voters voted for candidate A. This is not a breach of voter privacy, it is a simple logical deduction, and it would be utter nonsense for a county to say in this situation “We can’t release the election results because you could tell how people voted”! This would also violate another federal law, 52 U.S.C. § 10307, which under “Prohibited Acts” states “No person acting under color of law shall...willfully fail or refuse to tabulate, count, and report” the vote of any person “who is entitled to vote.”

There is, however, one situation which has recently been highlighted by a number of observers where transparency does result in an avoidable loss of voter privacy.

Example 3: In some counties there has been a move to countywide voting, where a voter is not required to vote in their precinct but may vote anywhere. Suppose a voter lives in the far southeast corner of the county (say precinct 29) but works in the far northwest corner of the county (say precinct 7) and decides to vote there for convenience. Because of the distance from their home precinct, it may happen that on that day (perhaps an early-voting day) this voter was the only one from that precinct to vote at that distant polling place. Then the register of voters at precinct 7 for that day would only have one voter from precinct 29 checked in, and the precinct number on the ballot that day would unavoidably identify the voter.

To prevent that, some have proposed deleting the precinct number from the election records, which would be a federal crime, violating 52 U.S.C. § 20702—much like using a sledgehammer to helpfully kill a mosquito on your friend's forehead and then going to prison for assault and battery and attempted murder. The flaw is in the use of countywide voting, which created the vulnerability. The precinct number is part of the federally-required CVR, and is also necessary for auditing (for example, to verify the number of votes in a precinct versus the number of registered voters in that precinct), and thus may not be deleted; otherwise, the voting system would not be completely auditable as required.

Finally, the courts have in fact already ruled on this potential conflict. In *Sewell v. Chambers*, 209 S.W.2d 363 (Tex. App. 1948), the court held that:

We have a wholesome rule of law that the secret ballot be not treated lightly. However, there are public interests which outweigh the individual's right to have his ballot kept secret. "The stability of our government is dependent upon the honesty and purity of the ballot[;] the secrecy of the ballot had better be scattered to the four winds, rather than have such secrecy shield corruption in elections, \* \* \* better a thousand times that the individual's vote should be spread upon canvas under calcium light, than that fraud should be locked up within the lids of official ballot boxes and poll books with no known legal method of exposing such fraud." *Gantt v. Brown et al.*, 238 Mo. 560, 142 S.W. 422, 425.

So where does that leave us? It boils down to this: (1) All election data needed for a complete forensic audit must be public and transparent, (2) but other than that, the county should protect voter privacy and ballot secrecy to the greatest extent possible, (3) except when the voter voluntarily divulges their vote. In summary, auditability of elections trumps ballot secrecy.