Ray Lutz
Executive Director, Citizens Oversight
https://citizensoversight.org
https://auditengine.org

raylutz@citizensoversight.org
619-820-5321 (mobile)
619-440-3646 (support)

Sept 5, 2024

(REF: M2023)

JOINT LETTER TO PRESIDENT BIDEN AND ATTORNEY GENERAL GARLAND

Subject: Ensuring Election Transparency and Compliance with Federal Law

Introduction:

The integrity and transparency of our elections is essential to public trust, while voter privacy is critical to preventing intimidation and coercion. However, some jurisdictions have been found to delete digital election records, like ballot images, which compromises auditability and violates federal law.

To address these issues, we urge your immediate attention to ensure the preservation of election records and to provide clear guidelines that balance transparency with voter privacy. Our recommendations aim to protect both the integrity of the electoral process and the privacy of individual voters.

Although we have made every effort to ensure that our requests align with the framework of the U.S. Constitution and the authority of federal and state agencies, we understand that practical constraints may arise. We ask that these requests be adapted in the most effective manner possible to achieve the intended outcomes, while respecting legal and operational limitations.

Executive Summary:

Section I:
Ballot images are created when paper ballots are scanned for tabulation by voting systems. These images are digital election records.

On July 28, 2021, the DOJ clarified that Section 301 of the Civil Rights Act of 1960 (codified at 52 U.S.C. §§ 20701-20706) requires retention and preservation of election records, including digital records, for 22 months. The DOJ explicitly stated that "election records" encompass digital and electronic records, mandating their preservation.[1]

However, some jurisdictions currently delete original ballot images, which is a clear violation of federal law and results in the loss of critical audit records.

We request that the President and the Department of Justice further clarify the 2021 statement to affirm that ballot images are digital election records that must be preserved. Destroying these images should be recognized as a violation of federal law.

Section II:
Achieving a balance between election data transparency and voter privacy is crucial. Transparency allows the public to verify election results independently, while voter privacy is essential to prevent coercion and intimidation. Our position is that both transparency and privacy can be nearly, though not always absolutely, assured. Ballot images, cast-vote records, and other election data are "designed-for-anonymity," meaning there is typically little to no risk to voter privacy even if these records are fully published. However, no system is perfect, and in some cases, withholding certain details may be necessary to protect voter privacy.

We also recommend clarifying voter intimidation laws to prevent the use of anonymous election data to reveal how any specific individual voted, especially in cases where design-for-anonymity is not foolproof. By clarifying existing retention and anti-intimidation laws, we aim to ensure that no coercion or intimidation occurs while promoting maximum transparency.

[1] https://www.justice.gov/media/1160831/dl

SECTION 1:
Stop Unlawful Deletion of Election Records

1. Durable Paper Ballots are Essential but Inaccessible

Hard evidence is crucial to confirm the accuracy of election results. Most jurisdictions now use **durable paper ballots**, which enable auditing, and if backed by securely transported and stored physical originals, provide a timely way of verifying election results by election officials. However, physical ballots are typically not available for the public to access, and election officials are auditing themselves, an obvious conflict of interest.

Paper ballots are often difficult or impossible for the public to access. Typically, they are sealed and stored immediately after the election, requiring a court order for inspection—a process that can be lengthy and uncertain. Additionally, these ballots may be destroyed after the federally mandated 22-month retention period.

While durable paper ballots are necessary for verifiable election outcomes, they do not provide the public with a timely or transparent mechanism for verification.

2. Today's Voting Systems Create Ballot Images

Modern voting systems first create a digital image of the paper ballot, which is then interpreted to determine voter intent and generate a digital summary of the votes cast, known as the "Cast Vote Record" (CVR). Each CVR is associated with a ballot number that can be matched to the corresponding ballot image.

When original ballot images are retained, they can be correlated with their respective CVRs, allowing for verification that voter intent was accurately captured. This process helps to prevent false claims of election hacking.

The original ballot image is not transient or redundant; it is a critical election record that must be preserved. Deleting these images hinders the ability to conduct precise audits. Original ballot images are irreplaceable; rescanning ballots cannot substitute for retaining the original images, as new images cannot be directly matched with the original CVRs. Deleting original images destroys essential auditing information[2].

[2] If original ballot images are deleted after ballots are rescanned, the rescanned images can only be compared to the results reported by groups (such as precincts, split precincts, or consolidated precincts, possibly further divided by early votes, election day, mail-in votes, etc.). If the totals for a reported group do not match exactly, identifying the specific ballot with the discrepancy becomes challenging within the group. With original images retained, the exact image with the discrepancy can be found and adjudicated. Moreover, not all

If ballots are rescanned, the new data must also be preserved. However, rescanned images cannot replace original ballot images because they will not correlate with the original CVRs. Only the original images provide this necessary correlation.

3. Retaining Digital Records Presents No Significant Hardship

Some jurisdictions that delete original ballot images argue that retaining them is too difficult or costly. However, the evidence does not support these claims.

Negligible Storage costs: Unlike paper ballots, which require secure physical storage, the cost to retain digital records is minimal. For example, assuming 150 million ballots are cast nationally, and each image consumes 300KB, the total storage required would be about 45TB. This amount of data could be stored on-line for less than $50/month[3]. As digital storage costs have declined exponentially since the 1950s[4], there is no reason to believe this trend will not continue.

Negligible Time costs: There may be complaints that it takes too long to save the images. Indeed, with current ES&S voting systems, there appears to be an additional approximately 10 minutes in the closing time of an average precinct[5]. However, other voting systems always save images and show no time difference because they cannot delete images at the machine level. With advances in technology and improved data storage devices, any time difference will likely become negligible. By mandating the retention of these images, voting systems will adapt to save them more efficiently.

---

discrepancies are apparent in the precinct totals, such as cases where one error offsets another. Conducting a ballot-by-ballot comparison, which is feasible with original images, enables software to minimize the number of ballots that require manual review for ambiguities. This process makes it easier to focus on the images in question and, if necessary, access the corresponding paper ballots for further comparison.

[3] Based on the cost of storing 50TB on AWS s3 "deep glacier" tier. However, the federal government no doubt has their own servers that can be used at lower cost.

[4] "In the last 70 years, the price for a unit of storage has fallen by almost ten orders of magnitude." https://ourworldindata.org/data-insights/the-price-of-computer-storage-has-fallen-exponentially-since-the-1950s

[5] From research done in Miami-Dade where the machines were actually timed, resulting in about 0.42 second additional time per ballot sheet for saving all ballot images.

4. Digital Records must be Retained, according to existing law

As mentioned in the Executive Summary, in 2021 the DOJ clarified that digital records must be retained[6], (extract, underlining added):

> The Civil Rights Act of 1960, now codified at 52 U.S.C. §§ 20701-20706, governs certain "[f]ederal election records." Section 301 of the Act requires state and local election officials to "retain and preserve" all records relating to any "act requisite to voting" for twenty-two months after the conduct of "any general, special, or primary election" at which citizens vote for "President, Vice President, presidential elector, Member of the Senate, [or] Member of the House of Representatives," 52 U.S.C. § 20701. 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.

5. Many Election Districts Routinely And Unlawfully Delete Ballot Images Created By The Voting System[7]

Despite federal requirements, some jurisdictions continue to delete original ballot images. This may be due to a lack of attention to federal law or to the DOJ's 2021 clarification. Some officials have argued that ballot images are transient data, falling outside the legal definition of "records," and therefore subject to deletion.

The act of deleting ballot images can itself fuel conspiracy theories. Even if these images are only accessible by court order, retaining them can help prevent misinformation and false claims. As discussed in Section 2, below, making these images available to civic groups, news organizations, and political parties would improve voter confidence and should be encouraged.

[6] https://www.justice.gov/media/1160831/dl

[7] For example, in Florida, many districts have argued in court that the ballot images are transient information that need not be saved, and therefore routinely delete these images. In Fulton County, Georgia, in the 2020 election, 380,458 original images were deleted, even though the paper ballots and images created in the recount were not deleted. See "2020 Election Ballot Image Audit of Fulton County GA", Page 2 -- https://copswiki.org/w/pub/Common/M1986/GA%20Fulton%2020201103%20Narrative%20Report.pdf

6. Therefore, please Clarify: Existing Law Must be Followed

REQUEST 1 (DOJ):

The DOJ should further clarify its 2021 guidance, affirming that ballot images are digital election records that must be preserved and retained for at least 22 months, and that their destruction violates federal law.

REQUEST 2 (PRESIDENT):

We urge the President to direct the Department of Justice to issue clear guidance to all state and local election officials on the federal requirements for retaining digital election data, including original ballot images. Furthermore, we encourage the President to work with Congress to pass legislation that explicitly mandates the retention of this critical election data, ensuring transparency and accountability in our electoral process.

REQUEST 3 (EAC):

Since deleting ballot images is unlawful, the Election Assistance Commission (EAC) should revise the Voluntary Voting System Guidelines to prohibit voting system vendors from offering machines that automatically delete ballot images.

SECTION 2:
Securing and Publishing Election Data

7. Section 2 Introduction:

Achieving a balance between election data transparency and voter privacy is crucial. Transparency allows the public to verify election results independently, while voter privacy is essential to prevent coercion and intimidation.

Our position is that both transparency and privacy can be nearly, though not always absolutely, assured. Ballot images, cast-vote records, and other election data are "**designed-for-anonymity**," meaning there is typically little to no risk to voter privacy even if these records are fully published. However, no system is perfect, and in some cases, withholding certain details may be necessary to protect voter privacy.

We also recommend clarifying **voter intimidation laws** to prevent the use of anonymous election data to reveal how any specific individual voted, especially in cases where design-for-anonymity is not foolproof.

We believe our recommendations align with the goals of other groups concerned with this issue[8], but our approach is more concrete and actionable. By clarifying existing retention and anti-intimidation laws, we aim to ensure that no coercion or intimidation occurs, while promoting maximum transparency.

8. Oversight Of Our Elections Is A Citizen Responsibility

As Supreme Court Justice Louis D. Brandeis famously said:

> "The most important political office is that of the private citizen."

We should not dismiss all inquiries into the accuracy of election results as "election denial." Instead, we should celebrate public involvement in providing necessary oversight. Legitimate concerns about election results often stem from mistakes, such as misconfigurations, aggregation errors, software inadequacies, or operator errors. While these mistakes rarely change the outcome, they do occur.

Our government cannot oversee itself; that is ultimately the role of citizens in a democracy.

---

[8] League of Women Voters (LWV) of Texas & others are concerned about a) not retaining election data and b) the potential for intimidation or coercion if voters are linked to their ballots.
https://southerncoalition.org/wp-content/uploads/2024/06/Texas-Ballot-Secrecy-6.13.2024.pdf

To prevent misinformation, conspiracy theories, and false claims, election data designed for anonymity should be treated as public records and not exempt from disclosure. The principle of "trust but verify" is essential. We believe that when all evidence is accessible and examined, true election denial will not persist because the public can verify the results for themselves.

9. Ballots and Ballot Images are Anonymous-by-Design

Modern paper ballots and their corresponding ballot images are designed to ensure anonymity, meaning that they do not reveal the identity of the voter. This design is crucial for maintaining voter secrecy and privacy. Once a ballot leaves a voter's hands or is removed from a mail ballot return envelope, there is nothing that directly ties that ballot to a voter.

- **Privacy** refers to the right of individuals to control their personal information and prevent unauthorized access. In the context of voting, privacy ensures that personal details about the voter are kept confidential and not disclosed without their consent.

- **Secrecy** pertains specifically to keeping the content of a voter's choices undisclosed. It ensures that how an individual voted is not revealed to others, protecting the voter from coercion and maintaining the integrity of the electoral process.

- **Anonymity** is about concealing the voter's identity in relation to their ballot. Ballots and ballot images are created to prevent any linkage between the voter's identity and their voting choices, thus safeguarding against any potential misuse of their voting behavior.

Despite these protections, in very rare cases, the votes of individual voters might be inferred through cross-referencing with other information, particularly in districts with overlapping boundaries or small voting groups. However, research[9] shows that the fraction of ballots that can be linked to specific voters is extremely small, especially when there is no direct linkage of voters to their ballots and when precincts are large enough to avoid small groupings[10].

---

[9] "The Still Secret Ballot: The Limited Privacy Cost of Transparent Election Results" -- https://arxiv.org/abs/2308.04100

[10] Similarly, if the district has very few voters classified into many groups, then the fraction of voters that might be revealed may be a relatively large fraction of the total, even when ballot images and cast vote records are not available. In such cases, the size of groups should be

If districts choose to use very small precincts and report on all groups (such as early voting, election day, and mail-in ballots), especially in primary elections where different parties have distinct ballots, meeting all the constraints may become challenging. This is particularly true if the state imposes high minimum requirements for the number of ballots in each anonymizing group (for example, Florida requires 30 ballots per group). To address these challenges, it may be necessary to consolidate precincts, reduce the number of reporting groups, and use separate ballot styles only when contest differences justify it. Additionally, states may need to reconsider and reduce statutory requirements for the minimum number of ballots per group (10 might be more reasonable)[11].

However, we believe that protecting how voters voted should not rely solely on perfecting anonymization. It is also essential to legally restrict the disclosure of voting choices by strengthening voter intimidation prohibitions.

10. Existing law prohibits intimidation and coercion

Federal law prohibits intimidating voters.[12] In theory, this makes it unnecessary to redact ballot images for the instances when additional information (beyond ballot images and cast vote records) might be used to identify a voter or determine their vote if they are part of a small group with a uniform vote. Given that intimidation is already illegal, one could argue that there is no need for further redaction of ballot

---

increased and adjacent districts merged.

[11] Technical Report: 100% Retabulation Audits: 2022 Primary and General Election Audit Data and Ballot Images from Leon County, FL
https://2022voterdata.lci.fsu.edu/wp-content/uploads/2023/10/Technical_Report_LA4.pdf

[12] For example, Section 11(b) of the Voting Rights Act of 1965 provides that "No person, whether acting under color of law or otherwise, shall intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for voting or attempting to vote, or intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for urging or aiding any person to vote or attempt to vote...." 52 U.S.C. § 10307(b). Similarly, Section 12 of the National Voter Registration Act of 1993 makes it illegal for any person, "including an election official," to "knowingly and willfully intimidate[], threaten[], or coerce[], or attempt to intimidate, threaten, or coerce, any person for . . . registering to vote, or voting, or attempting to register or vote" in any election for federal office. Id. § 20511(1)(A). Likewise, Section 131 of the Civil Rights Act of 1957 provides that "[n]o person, whether acting under color of law or otherwise, shall intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce any other person for the purpose of interfering with the right of such other person to vote or to vote as he may choose, or of causing such other person to vote for, or not to vote for, any candidate" for federal office. 52 U.S.C. § 10101(b).

images[13].

However, there is a legitimate debate over whether personally identifiable information (PII), such as signatures or social security numbers, must be redacted from ballots. While voters are generally not allowed to add distinguishing marks to their ballots, and thus cannot claim these marks as a basis for redaction, such marks could potentially be used to identify a ballot. Therefore, it is prudent to redact any PII to safeguard privacy.

In cases where voters are in very small groups (e.g., a single voter in a precinct), withholding ballots from these small groups might be sufficient to preserve voter privacy while still allowing for transparency. This approach would maintain the integrity of the audit process, as withholding a few ballots from disclosure rarely significantly impacts auditing accuracy. For closely contested elections, any withheld ballots can be reviewed under court order if necessary.

11. The intimidation prohibition needs clarification

Federal laws prohibiting voter intimidation are currently too vague concerning the exposure of how an individual voted. While voters are free to disclose their own voting choices, revealing how others voted without their permission constitutes voter intimidation. However, because of the freedom of speech, it is challenging to completely ban claims about how someone voted. Therefore, we believe it is necessary to make it illegal to use anonymous election data to demonstrate how any voter voted.

Intimidation may not always be direct but could manifest as a general deterrent if voters believe that their votes can be identified from published data.

REQUEST 4A (DOJ):

The DOJ should provide further clarification on the prohibition of voter intimidation. We suggest the following:

> *It should be considered voter intimidation to use election data, such as ballot images and cast vote records, to reveal how any specific voter(s) voted. Researchers are still permitted to report on the vulnerabilities of ballot anonymity to officials, which can lead to improvements in data*

[13] Although no redaction is our preference, a small set of withheld ballot images and corresponding cast vote records will still allow ballot image audits to take place if the totals of the withheld ballots are provided.

privacy. However, these reports should not disclose how individual voters voted.

12. Districts Must Not Explicitly Link Voters to Their Ballots

Certain states **explicitly maintain data that links voters to ballots,** often by using identifiable descriptors on ballots, as seen in recent cases in Texas[14]. This practice is different from the rare instances where individual ballots might be revealed through triangulation of other information. By correlating descriptors, all voters on the list are at risk of having their ballot choices exposed.

States[15] like Texas and North Carolina,[16] require "ballot retrieval" processes, which allow for the identification and removal of a specific voter's ballot from further processing. This means that each ballot can be traced back to the voter who completed it, potentially exposing the votes of all voters if such data is misused.

If malicious or compromised officials gain access to this data, they could potentially sell or release the voting choices of all individuals. This constitutes a form of voter intimidation, even if no explicit threats are made and even if such data is not used. This risk is particularly significant if political parties could exploit such information to instill fear and coerce voters. Therefore, linkages that directly connect voters to their ballots must be eliminated.

---

[14] https://www.texastribune.org/2024/06/06/texas-voting-ballot-secrecy-public-records-elections/

[15] At least 11 states — nine by statute and two based on attorney general opinions — prohibit counting votes from absentee voters who cast a ballot, then die before Election Day, while nine states specifically allow it, according to the National Conference of State Legislatures.

[16] NC Gen Stat §163-227.5. "One-stop voting counties having voting systems with retrievable ballots" describes how voters can cast their vote and it may be later retrieved "The plan shall provide that each one-stop ballot shall have a ballot number on it in accordance with G.S. 163-230.1(c), or shall have an equivalent identifier to allow for retrievability."

G.S. 163-230.1(c) provides:
(1) On the top margin of each ballot the applicant is entitled to vote, the chair, a member, officer, or employee of the board of elections shall write or type the words "Absentee Ballot No. ____ " ... and insert in the blank space the number assigned [to] the applicant's application.... Alternatively, the board of elections may cause to be barcoded on the ballot the voter's application number, if that barcoding system is approved by the State Board. https://law.justia.com/codes/north-carolina/chapter-163/article-20/section-163-230-1/

Instead, such late applications for absentee voting can be held in sealed envelopes until after the voter has been approved, and then the ballot can be processed anonymously, without any identifier. Voters who die after voting but before election day may be now retrieved and removed but those are very few and are not worth the risk of providing for retrievable ballots.

REQUEST 4B (DOJ):

The DOJ should clarify the prohibition on voter intimidation to include the following:

> *Any direct linkage of ballots to specific voters, such as maintaining lists that connect ballots to voter identities, is considered a form of voter intimidation and is unlawful, even if officials assert that the information will be kept confidential.*

Consequently, systems that allow for retrieving ballots by voter identification or through intermediate lists, such as absentee application lists, should be prohibited.

While implementing this change may be challenging before the 2024 election, it should be a long-term goal to ensure robust protection against voter intimidation.

13. Many Jurisdictions Already Publish Data

While the use and retention of durable paper ballots are crucial for election integrity, providing public access to digital records of designed-to-be-anonymous election data is equally important. Open government initiatives support transparency[17] through electronic records, and many jurisdictions are recognizing the value of publishing comprehensive election data, including ballot images and cast vote records.

Secretaries of State across the country now accept electronic records as legal substitutes for paper records[18]. Several jurisdictions have begun to make extensive election data publicly available, which can significantly reduce the administrative burden associated with public records requests.

---

[17] The Obama administration started an initiative to move to electronic records and emphasized the desire for open government and access to those records when appropriate by the public and specified "transitioning from paper-based records management to electronic records management where feasible." https://obamawhitehouse.archives.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records

[18] "Digital documents, when created and maintained in a trusted system that ensures their integrity, authenticity, and accessibility, have the same legal standing as paper documents." -- this statement reflects the principles outlined in Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Uniform Electronic Transactions Act (UETA), and is generally recognized by secretaries of state and court precedents, such as *Lorraine v. Markel American Insurance Co. (2007), U.S. v. Kahre (2009),* and *U.S. v. Cone (2010).*

Examples of Jurisdictions Publishing Data:

- **San Francisco, CA** -- Since at least 2020, San Francisco County has been publishing ballot images, cast vote records, and other relevant election data. They do redact personal or distinctive information as needed, but this has not diminished the utility of the data.

- **Dallas, TX:** For the March 2024 primary election, Dallas released a comprehensive set of data, including images of voting machine "poll tapes," which show aggregated totals for each machine. This extensive publication marks a significant step forward in Texas[19].

  We were impressed to see the inclusion of images of voting machine "poll tapes" which provide the aggregated totals for all ballots processed on each machine. The recent disputed election in Venezuela included the use of scanned machine tapes, demonstrating their usefulness[20].

- **Dane County, WI:** Dane County has been a leader in posting nearly all ballot images since 2016, without redaction.[21]

- **Maryland:** Maryland provides ballot images and cast vote records for recent elections and responds to public records requests with transparency.

Currently, while some records are accessible under public records laws, the costs and process can be burdensome for requesters and election administrators alike. Publishing ballot images and cast vote records proactively can reduce these costs and streamline access to information.

---

[19] https://mailchi.mp/dallascounty/presser_openelectionrecords

[20] Scans of "tally sheets" (poll tapes) were critical in demonstrating the outcome of this election. These poll tapes include QR Codes that make it easier to collect data from the approximately 30,000 machines. https://apnews.com/article/venezuela-election-maduro-machado-edmundo-chorizo-6d9f3999c60c09eb30e69c757ce80b11

[21] Dane County provides instructions for a "Do It Yourself Audit" on this page: https://elections.countyofdane.com/Auditing (WI does have a law that voter identification numbers of some voters must be added to the back of those ballots and then a small number of ballots must be withheld because they have these numbers and can be linked to those voters. This law should be modified to avoid placing these voter id numbers on ballots.)

REQUEST 5 (PRESIDENT):

The President should initiate a project (probably conducted by NIST) to

a) Standardize the storage and organization of ballot images, machine reports, and other election data to ensure they are easily accessible to the public.

b) Define clear guidelines for any necessary redactions to maintain voter privacy while promoting transparency.

The findings of this project should be provided to states as recommendations to enhance consistency and accessibility across jurisdictions.

14. Improve Ballot Image Security

For ballot images to be trusted, they must be authentic and protected against tampering. Research has shown that ballot images can be maliciously altered,[22] highlighting the need for robust measures to ensure their integrity. The traceability of ballot images, or their provenance, can be significantly enhanced by leveraging new standards and technologies developed to track digital assets such as photos, videos, and documents.

Advancements in Digital Provenance:

- **Coalition for Content Provenance and Authenticity (C2PA)[23]:** This organization is developing technical standards to certify the provenance of digital media, primarily photographic and video content. These standards help differentiate genuine content from AI-generated or manipulated material. The C2PA's approach includes digital mechanisms for tracking the edits and redactions applied to original data, providing a comprehensive audit trail.

- **Cryptographic Mechanisms:** Utilizing conventional cryptographic techniques, digital signatures can be applied to ballot images, making it virtually impossible to alter or fabricate ballot data without detection.

[22] See https://mbernhard.com/papers/unclearballot.pdf "UnclearBallot: Automated Ballot Image Manipulation". Also see: https://copswiki.org/Common/M1976 'Critical Review of 'Unclear ballot'"

[23] https://c2pa.org/ -- Coalition for Content Provenance and Authenticity

15. Recommendations for Ballot Image Protection:

Collaboration with Industry Standards:

- The National Institute of Standards and Technology (NIST) should work with C2PA and other relevant industry initiatives to develop and prescribe detailed procedures for the protection of ballot images and other election data. This includes implementing cryptographic security measures and ensuring the authenticity and integrity of retained federal election data.

Incorporation into Voting System Guidelines:

- The Election Assistance Commission (EAC) should incorporate these procedures into the Voluntary Voting System Guidelines (VVSG). This will make it likely that new voting machines include the necessary capabilities for securing and authenticating ballot images[24].

Redaction and Provenance Tracking:

- C2PA's digital mechanisms for editing and redaction should be utilized to track and roll back changes when personal information needs to be redacted from ballot images. These mechanisms ensure that redactions are transparent and verifiable without exposing the original data.

Exploring Zero-Knowledge Proofs:

- The industry is also exploring "zero-knowledge" proofs, which can validate the legitimacy of an image without revealing the original[25] or the content behind redactions. While these proofs are still emerging and may not be feasible for immediate implementation, they represent a promising direction for future ballot image security[26].

---

[24] https://copswiki.org/w/pub/Common/M1998/COPS%20VVSG%202.0%20Comments%20(M1998).pdf -- Comments on VVSG 2.0, including recommendations for improving data cybersecurity, submitted by Ray Lutz and Citizens Oversight 2023-06-07, although it did not stress the adoption of C2PA approach.

[25] https://www.di.ens.fr/~nitulesc/files/Survey-SNARKs.pdf -- "zk-SNARKs: A Gentle Introduction" (A SNARK provides a way to prove, without reference to any other information, that the data protected is legitimate.

[26] The editor of this letter, Ray Lutz, can assist in this direction as he has been involved in the development of cryptographic procedures and has submitted these suggestions as

REQUEST 6 (PRESIDENT):

The President should request that NIST and the Election Assistance Commission jointly develop and implement standards and procedures for cryptographic security of ballot images and other election data. This should be done in collaboration with industry initiatives such as C2PA to ensure full authentication, including verification of any edits and redactions.

16. Let's Get Serious: Permanent Archival

The cost of retaining digital records is minimal compared to the expense of storing physical paper records. Given their significance in documenting our democratic process, digital election records should be preserved permanently as a vital aspect of our historical archive.

Rationale for Permanent Digital Archival:

- **Cost Efficiency:** The expense of maintaining digital records is negligible compared to physical storage costs. Digital records are more durable and easier to manage, making them a cost-effective choice for long-term preservation.

- **Historical Significance:** Election data is a crucial part of our national history. Permanent archival ensures that this data remains accessible for future generations, supporting historical research and maintaining transparency about our electoral processes.

- **Reduction of Public Records Requests:** By making election data available for comprehensive public review, the burden on election officials to handle numerous public records requests is alleviated. This proactive approach not only streamlines access to information but also reduces the workload and associated costs for election offices.

Recommendations for Permanent Archival:

Collaboration with Key Institutions:

- The Election Assistance Commission (EAC), in conjunction with the National Archives and Records Administration (NARA) and the Library of Congress, should take responsibility for the permanent archival of

---

comments to the Voluntary Voting System Guidelines (VVSG) managed by the Election Assistance Commission (EAC). (see "Comments on VVSG 2.0" above).

digital election records. These institutions have the expertise and infrastructure to manage and preserve important national records.

Comprehensive Public Access:

- Ensure that digital election records are made available for full public review to the greatest extent possible. This transparency supports accountability and reduces the administrative burden associated with processing individual public records requests.

REQUEST 7 (PRESIDENT):

The President should issue an executive order mandating that digital records of federal elections be permanently archived. This should be done in coordination with the Election Assistance Commission, the National Archives and Records Administration (NARA), and the Library of Congress, to ensure that this critical historical data is preserved and accessible for future generations.

Conclusion

In summary, please accept and implement these recommendations using the best mechanisms available.

FOR THE DOJ:

REQUEST 1 (DOJ):

The DOJ should further clarify its 2021 guidance, affirming that ballot images are digital election records that must be preserved and retained for at least 22 months, and that their destruction violates federal law.

REQUEST 4A (DOJ):

The DOJ should further clarify the intimidation prohibition:
It is prohibited voter intimidation to use election data, such as ballot images and cast vote records, to prove how any voter(s) voted. Researchers can, however, provide reports of weaknesses of ballot anonymity to officials to allow them to redact or withhold data to resolve privacy concerns, and to prompt improvement in anonymity of the data for the future, but these reports should not provide the votes of any specific voters.

REQUEST 4B (DOJ):

The DOJ should clarify the intimidation prohibition: Any direct linkage between voters and their ballots is considered a form of voter intimidation and is unlawful, even if officials claim the information will be kept secret.

FOR THE PRESIDENT:

REQUEST 2 (PRESIDENT):

We urge the President to direct the Department of Justice to issue clear guidance to all state and local election officials on the federal requirements for retaining digital election data, including original ballot images. Furthermore, we encourage the President to work with Congress to pass legislation that explicitly mandates the retention of this critical election data, ensuring transparency and accountability in our electoral process.

REQUEST 5 (PRESIDENT):

The President should initiate a project (probably conducted by NIST) to

a) Standardize the storage and organization of ballot images, machine reports, and other election data to ensure they are easily accessible to the public.

b) Define clear guidelines for any necessary redactions to maintain voter privacy while promoting transparency.

The findings of this project should be provided to states as recommendations to enhance consistency and accessibility across jurisdictions.

REQUEST 6 (PRESIDENT):

The President should request that NIST and the Election Assistance Commission jointly develop and implement standards and procedures for cryptographic security of ballot images and other election data. This should be done in collaboration with industry initiatives such as C2PA to ensure full authentication, including verification of any edits and redactions.

REQUEST 7 (PRESIDENT):

The President should issue an executive order mandating that digital records of federal elections be permanently archived. This should be done in

coordination with the Election Assistance Commission, the National Archives and Records Administration (NARA), and the Library of Congress, to ensure that this critical historical data is preserved and accessible for future generations.

PROPOSED PRESIDENTIAL ORDER:

The President should direct relevant federal agencies, including the Department of Justice (DOJ), the National Institute of Standards and Technology (NIST), and the Election Assistance Commission (EAC), to collaborate with state and local election officials on the following recommendations to enhance the integrity and transparency of federal elections:

1. **Retention of Ballot Images:**
   The DOJ should issue clear guidance on the importance of retaining original and any subsequent ballot images of all paper ballots, where voting systems have the capability to create such images. While respecting state and local authority over elections, the federal government should encourage jurisdictions to adopt best practices for data retention.

2. **Improving Ballot Anonymity:**
   The EAC should provide states with best practices to ensure ballot anonymity, such as avoiding any linkage between voters and their ballots. For example, ballots should not be numbered in a way that links them to voter records or other lists that could compromise voter privacy.

3. **Reporting Practices:**
   The EAC should offer guidance on the reporting of election results, particularly to avoid the identification of small voter groups in reports, such as those related to federal-only ballots, which could risk voter privacy.

4. **Public Access to Election Data:**
   The EAC should develop standards to help states and localities make ballot images, cast vote records, and other reported data available for public review without cost. These standards should encourage the publication of such data on relevant government websites or data portals to streamline public access and minimize delays in fulfilling public records requests.

5. **Archiving Federal Election Data:**
   The EAC, in conjunction with the National Archives and Records Administration (NARA) and the Library of Congress, should work with state and local governments to ensure the permanent archiving of digital records

from federal elections, thereby preserving the historical record.

6. **Cryptographic Security Standards:**
   NIST, in collaboration with the EAC and industry initiatives like the Coalition for Content Provenance and Authenticity (C2PA), should develop and recommend standards and procedures for implementing cryptographic security for ballot images and other election data. These standards would allow for full authentication of images, including verification of any edits and redactions, while maintaining the integrity of the data.

7. **Redaction of Ballot Images:**
   The EAC should clarify whether any redactions to ballot images are necessary to maintain transparency while ensuring the full privacy of voters. This guidance should balance the need for public access to election data with the protection of voter anonymity.

FOR THE ELECTIONS ASSISTANCE COMMISSION (EAC):

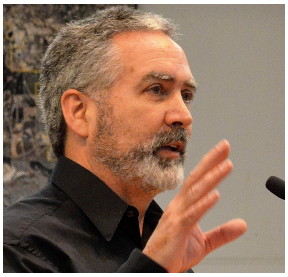
REQUEST 3 (EAC):

Since deleting ballot images is unlawful, the EAC should revise the Voluntary Voting System Guidelines to recommend that voting system vendors stop offering machines that automatically delete ballot images.

Please support the election integrity community by issuing these orders as soon as possible. These actions will demonstrate your administration's commitment to a fair, transparent, and evidence-based election process.

Sincerely,

Ray Lutz, Executive Director, CitizensOversight
Creator of "AuditEngine", a ballot image auditing solution



Primary Author: Raymond Lutz

Raymond Lutz is the founder and executive director of Citizens' Oversight Projects, a 501(c)(3) nonpartisan nonprofit organization that has been involved in providing oversight to elections for over 15 years. Lutz has a Masters degree in

electronics and software engineering, with experience in the document management and printer/scanner/fax/copier industry, and medical device industry. He is the lead developer of AuditEngine, and was a congressional candidate in 2010 for the CA-52 Congressional District.

COSIGNERS

Mimi Kennedy, Actor and Election Integrity Activist
John R Brakey, Co-founder & Director of AUDIT (Elections) USA, Tucson, AZ
Jan BenDor, Michigan Election Reform Alliance (MERA)
Darlene Little; Scrutineers, Protect California Ballots, and election integrity advocate since 2005.
Marta Steele, EI activist since 2001, OpEdNews.com
Bob Stromberg, Round Lake, NY
Celeste Landry, Boulder, CO, registered volunteer lobbyist on CO election bills
Daniel H. Wolf, Esq, CEO, Democracy Counts, Inc, San Diego, CA
Dale Axelrod, Sonoma County Democratic Party
Jim Soper, National Voting Rights Task Force
Dale R. Tavris, MD, MPH, Orange Co. FL Democratic Party, Scrutineer (national election integrity organization)
Mark Demo, Citizens for New Jersey Election Integrity
Susan Pynchon, Florida Fair Elections Coalition
Douglas A. Kellner, Co-Chair, New York State Board of Elections (retired)
Jamie M. Friend, Founder & Chair, Citizen's Audit Broward, Hollywood, FL
Alan Minsky, Executive Director, Progressive Democrats of America (PDA)

DISTRIBUTION LIST

To be sent to:

President Biden
president@whitehouse.gov

Merrick Garland, DOJ
c/o Tamar Hagler
Voting Section
Civil Rights Division
4CON – Room 8.1136
950 Pennsylvania Avenue,
NW Washington, DC 20530
tamar.hagler@usdoj.gov

Also to:

U.S. Election Assistance Commission
Benjamin Hovland, Chair
633 3rd Street NW, STE 200
Washington DC 20001
submitted via website: https://www.eac.gov/contactuseac

NIST
Dr. Laurie E. Locascio, Director
National Institute of Standards and Technology
100 Bureau Dr
Gaithersburg MD 20899
laurie.locascio@nist.gov

National Assn of Secretaries of State
Hon. Steve Simon, President
National Association of Secretaries of State
444 North Capitol St NW, STE 401
Washington DC 20001
nass@nass.org

National Assn of AGs
Brian Kane, Executive Director
National Association of Attorneys General
1850 M Street NW, 12th floor
Washington DC 20036
support@naag.org

National Governors Association
Governor Jared Polis, Chair
National Governors Association
444 N Capitol St NW, STE 267
Washington DC 20001
info@nga.org

National Association of Election Officials
Kathleen Hale, JD, PhD, Executive Director
Election Center, National Association of Election Officials
403 W Grand Pkwy S, STE F #404
Katy TX 77494
services@electioncenter.org
https://www.electioncenter.org/certified-elections-certifications.php

Charles Stewart III, PhD, Founding Director
MIT Election Data & Science Lab (https://electionlab.mit.edu)
77 Massachusetts Ave
Cambridge MA 02139
mitelectionlab@mit.edu

Paige Alexander, CEO
The Carter Center
43 John Lewis Freedom Parkway NE
Atlanta GA 30307-1406
info@cartercenter.org

Harri Hursti
HackingDemocracyFilm@gmail.com

Free Speech for People
Susan Greenhalgh
https://freespeechforpeople.org/

CISA (Cybersecurity and Infrastructure Security Agency)
SayCISA@cisa.dhs.gov
Central@cisa.dhs.gov

Joyce LeBombard, President
League of Women Voters Texas
1212 Guadalupe St #107
Austin TX 78701
president@lwvtexas.org

Celina Stewart, LWVUS CEO
Caren E. Short, Legal & Research
League of Women Voters of the United States
1233 20th St NW, STE 500
Washington DC 20036
lwv@lwv.org

Chioma Chukwu, Interim Executive Director
American Oversight
1030 15th St NW, STE B255
Washington DC 20005
info@americanoversight.org

Chris Shenton
Southern Coalition for Social Justice
PO Box 51280
Durham NC 27717
media@scsj.org

Kate Huddleston, Senior Legal Counsel
Campaign Legal Center
1101 14th St NW, STE 400
Washington DC 20005
media@campaignlegal.org

Vice President Kamala Harris
https://kamalaharris.com/contact-us/

Former President Donald Trump
https://www.45office.com/info/share-your-thoughts