

## MIT Open Access Articles

### *When Is an Election Verifiable?*

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

**Citation:** Rivest, Ronald L. and Philip B. Stark. "When Is an Election Verifiable?" IEEE Security and Privacy 15, 3 (June 2017): 48-50 © 2017 IEEE

**As Published:** <http://dx.doi.org/10.1109/msp.2017.78>

**Publisher:** Institute of Electrical and Electronics Engineers (IEEE)

**Persistent URL:** <https://hdl.handle.net/1721.1/123682>

**Version:** Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

**Terms of use:** Creative Commons Attribution-Noncommercial-Share Alike



**Massachusetts Institute of Technology**

## *Electronic Voting*

# When Is an Election Verifiable?

Ronald L. Rivest | MIT

Philip B. Stark | University of California, Berkeley

***Verifiable elections currently require voter-verifiable paper ballots, demonstrably adequate custody of those ballots, and well-designed audits of the results based on manual inspection of those ballots.***

For years, election integrity advocates have called for voter-verified paper ballots: paper is tangible, tamper-evident, and readable and countable by humans without relying on software. But if laws and partisan wrangling make it impossible to use ballots to check the accuracy of electronically tabulated results, what good is the paper? Despite the proliferation of voting systems that use voter-verifiable paper as the ballot of record, the 2016 US presidential election and its aftermath—which included public demands to audit the results and legal battles over recounting the results in three states—make it clear that having an auditable paper record of voter intent falls far short of having verifiable elections.

US voting systems are vulnerable to error, misconfiguration, and hacking. At some point in each election cycle, most systems are either connected to the Internet directly or connected to other machines that have been connected to the Internet (through the exchange of removable media). Current election regulations don't provide adequate safeguards to detect problems, much less correct them—even though routine, rigorous statistical tabulation audits could do that job for systems with a voter-verifiable paper trail.

One wonders whether we can do better

- when a candidate asserts that “the election is rigged”;
- when suspicions mount that foreign actors might have manipulated the results;
- when margins are comparable to the counting technology’s intrinsic accuracy; and
- when states sue to stop efforts to ensure that election results are accurate.

The US is slowly unlearning bad habits and developing better practices for collecting votes. For instance, the paperless direct-recording electronic voting systems that proliferated after the Help America Vote Act of 2002 ([www.eac.gov/about/help-america-vote-act](http://www.eac.gov/about/help-america-vote-act)) are being phased out. In the 2016 election, approximately 80 percent of voters cast voter-verifiable paper ballots. This is substantial progress.

But while most US voters now use systems that produce a durable, tamper-evident, voter-verifiable, auditable record, our elections aren’t much more verifiable. The limiting factor is, by and large, not technical: it’s legal and political.

We've known for more than a decade that for elections to be verifiable, voting systems must be *software independent*:<sup>1</sup> it must not be necessary to trust a computer in order to trust the election outcome. Paper ballots provide a foundation for checking the work of computer systems used in elections, and allow voters to verify that their ballots are cast as intended. When appropriate procedures are used to ensure that the collection of cast paper ballots has integrity, recounts and audits in principle can verify and—if necessary—correct the reported election outcomes produced with computer assistance.

The last decade has also seen the development of efficient techniques for statistical error correction of election outcomes: *risk-limiting audits* that manually inspect randomly selected ballots to provide a guaranteed minimum chance of correcting incorrect outcomes.

A voting system should not only produce the correct election outcome but also produce evidence sufficient to convince losing candidates and their supporters that they lost the election fair and square. This evidence must convince the public as well, else we risk fostering mistrust both in the machinery of our democracy and in election outcomes. Such mistrust would engender apathy toward elections—or worse, a belief that changes in power should be effected by other means.

Software-independent systems based on paper ballots, sound procedures to protect and verify the audit trail's integrity, and risk-limiting audits of electronically tabulated results against the paper trail, represent today's best practice. Together, these comprise an evidence-based election system, where evidence = auditability + auditing.<sup>2</sup>

Unfortunately, best practice is not yet widely practiced. Colorado's elections will be evidence-based starting in late 2017, including mandatory risk-limiting audits relying on manual inspection of randomly selected paper ballots (Colorado Revised Statutes Title 1. Elections § Section 1-7-515). But most US jurisdictions with a paper trail don't use it to advantage for quality control and error correction.

We were disappointed that in the 2016 US presidential election, officials (and, by and large, the public) seemed unaware of the importance of using post-election audits or recounts to confirm that the announced winner really won. Perhaps worse, recount laws, as well as some candidates and election officials, actively stymied attempts to check the results. Verifying election outcomes should be routine best practice and good hygiene. As George Washington University computer science professor Poorvi Vora said, “Brush your teeth. Eat your spinach. Audit your elections.”<sup>3</sup>

Auditability, or verifiability, of election outcomes is perhaps the most important security requirement for voting systems. But auditability without auditing is toothless. Unless an audit or recount checks the outcome against a reliable paper trail, an election can be stolen in stealth by hackers from the other side of the planet. Verifying voters' eligibility and maintaining their privacy are important security goals, but their violation tends to allow the manipulation of vote counts by small amounts, rather than the stealing of elections wholesale.

We're pleased to see vigorous research on voting systems, including the papers in this

issue of *IEEE Security and Privacy* magazine. Innovative hybrid paper–electronic systems, such as the Secure, Transparent, Auditable, and Reliable (STAR)-Vote System being developed by Travis County, Texas, might eventually justify even higher levels of confidence than pure paper-based systems. Systems promising end-to-end verifiability (E2EV) are particularly promising. Even so, voting verifiably and anonymously over the Internet remains a distant dream—even applying E2EV principles is insufficient to make an Internet system trustworthy.<sup>4</sup>

Technology can be complex, and voting has severe requirements, with no parties who can be fully trusted. Keeping things simple, as with paper ballots, is exceptionally helpful in producing trustworthy voting systems. In every election, we must ask: What evidence does this voting system produce that its outcome is correct, and why should we believe it?

## References

1. R.L. Rivest and J.P. Wack, “On the Notion of ‘Software Independence’ in Voting Systems,” presentation to the Technical Guidelines Development Committee, 28 July 2006; people.csail.mit.edu/rivest/pubs/RW06.pdf. [//link OK?//](#)
2. P.B. Stark and D.A. Wagner, “Evidence-Based Elections,” *IEEE Security and Privacy*, vol. 10, no. 5, 2012, pp. 33–41.
3. A. Greenberg, “Hacked on Not, Audit This Election (And All Future Ones),” *Wired*, 23 Nov. 2016; www.wired.com/2016/11/hacked-not-audit-election-rest.
4. *The Future of Voting: End-to-End Verifiable Internet Voting—Specification and Feasibility Study*, report, US Vote Foundation and Galois, July 2015; www.usvotefoundation.org/sites/default/files/E2EVIV\_full\_report.pdf. [//link OK?//](#)

Ronald L. Rivest is an Institute Professor at MIT. His research interests include cryptography, election integrity, and algorithms. Rivest received a PhD in computer science from Stanford University. He's on the Board of Verified Voting Foundation and the EPIC Advisory Board. Contact him at rivest@mit.edu.

Philip B. Stark is professor of statistics and associate dean of mathematical and physical sciences at the University of California, Berkeley. His research focuses on uncertainty quantification and risk assessment in applications in physical, biological, and social sciences. Stark received a PhD in earth science from the University of California, San Diego. He's on the Board of Verified Voting Foundation and the US Election Assistance Commission's Board of Advisors. Contact him at stark@stat.berkeley.edu.

For our digital library:

**Abstract:** Truly verifiable elections will require software-independent systems based on paper ballots and risk-limiting audits of electronically tabulated results.

**Keywords:** elections, voting systems, end-to-end verifiable, verifiability, auditable, paper ballots, security, privacy