EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

Election Integrity in the United States: How Will 2024 Compare to 2020?

Hal Berghel, University of Nevada, Las Vegas

In this interview with Douglas Jones, we assess the integrity of the election infrastructure in the United States and compare the status with earlier assessments.

Douglas Jones is an emeritus professor in the Computer Science Department at the University of Iowa. He has been involved in voting technology research since 1995 and was a principal investigator for the National Science Foundation (NSF)-funded ACCURATE project (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections; accurate-voting.org). His book with coauthor Barbara Simons, *Broken Ballots: Will Your Vote Count?* (CSLI Publications, 2012),[16] is a seminal work in the area of current voting technology and is highly recommended to anyone who is concerned about election integrity at the ballot box.

This interview is the fourth that we've done with Doug on digital election equipment that we've published in *Computer* over the past decade or so. What follows resulted from our e-mail exchanges during May–July 2024. This is the fourth interview with Doug on this subject since 2016. (Note: Some of Doug's published work may be found online at http://homepage.cs.uiowa.edu/~dwjones/voting/.) Also, please see "Further Reading on Election Integrity" for additional resources concerning election integrity.

HAL BERGHEL: Let's pick up where we left off in our last interview in January 2022.[35] These were your concluding remarks.

> "I expect that the stop-the-steal movement will continue to challenge elections and push for roadblocks to voting for years to come. I also expect that local election jurisdictions will continue to be seriously underfunded and I expect the shortage of technically knowledgeable election staff to continue.

Digital Object Identifier 10.1109/MC.2024.3434190
Date of current version: 23 September 2024

Despite this dismal situation, some reforms are possible. I hope that more states will require such simple things as rudimentary inventory control and checklists to help reduce the incidence of chain-of-custody errors, double-counting of ballot batches, and ignored ballot batches. I hope more states require routine post-election audits, and among the states that audit, I hope that more of them will move toward more rigorous audits such as risk-limiting audits.

I don't expect anything rapid in the world of election technology. Voting equipment is built to last a decade or more, so even if we change our voting system requirements now, most of the hardware and software now in service will still be there in 4 years. On the other hand, we must find a way to update our requirements so that they take an end-to-end perspective on voting systems instead of merely focusing on the voting machine in the precinct, which is just one link in the chain from voter to the official election result."

It must be admitted that a stop-the-steal mantra was exceedingly serviceable in preparation for the subversion of the peaceful transfer of presidential power such as we witnessed on 6 January 2021. According to *The New York Times*, as of 3 January 2024, 720 of the 1,240 people arrested were sentenced for their involvement in the insurrection, and of those, 450 have been incarcerated.[1] Will these convictions rate impede future stop-the-steal initiatives?

DOUG JONES: No. Most of those arrested were followers, not leaders in the stop-the-steal movement. Furthermore, the promise of executive clemency for the convicts invites their allies to continued action.[2]

I attended Mike Lindell's August 2021 Cyber Symposium in Sioux Falls, SD, USA, where he promised to present incontrovertible evidence that the 2020 election had been rigged. None of the material presented at that meeting was convincing.[3,4] The news coverage of that event focused on the claims that Lindell and other speakers made about the stolen election, but numerous state legislators and other activists attended the meeting. As a result, the meeting served as an organizing event for the stop-the-steal movement, and it helped launch a long-running roadshow that went on to tour the country.[5] These events have helped build support for a wide-ranging legislative agenda that includes attempts to ban or severely limit early and absentee voting, require all voters to use hand-marked paper ballots, require hand counting of all ballots, require proof of citizenship to vote, and much more.

BERGHEL: In April 2023, just as opening arguments were scheduled to begin, Fox News settled a defamation suit with Dominion for US$787 million relating to their 2020 defamation suit against the network for propagating lies about Dominion's alleged "rigging" of the 2020 presidential election.[6] Dominion claimed US$1.6 billion in irreparable harm to its business over the false reporting. US$787 million is rising to the level of serious money. What, if any, effect will this judgment have on the future practice of election denial?

JONES: This and related lawsuits certainly put a damper on the activities of the major players in the 2020 election denial movement. People like Lindell and Giuliani have been far less visible

FURTHER READING ON ELECTION INTEGRITY

- A. Berman, *Give Us the Ballot: The Modern Struggle for Voting Rights in America, Picador Reprint*. Stuttgart, Germany: Pan Macmillan, 2016.
- J. Conyers and A. Miller, *What Went Wrong in Ohio: The Conyers Report on the 2004 Presidential Election*. Chicago, IL, USA: Academy Chicago Publishers, 2005.
- M. C. Miller, *Fooled Again: The Real Case for Electoral Reform*. New York, NY, USA: Basic Books, 2007.
- A. Rubin, *Brave New Ballot*. New York, NY, USA: Broadway, 2006.
- T. Campbell, *Deliver the Vote: A History of Election Fraud, an American Political Tradition – 1742–2004*. New York, NY, USA: Carroll and Graf, 2004.
- J. Serebrov and T. Wang, "Voting Fraud and Voter Intimidation, Report to the U.S. Election Assistance Commission on Preliminary Research and Recommendations," *New York Times*, Apr. 2007. Accessed: Jul. 1, 2024. [Online]. Available: https://graphics8.nytimes.com/packages/pdf/national/20070411voters_draft_report.pdf
- T. Wang and J. Nittoli, *The Politics of Voter Suppression: Defending and Expanding Americans' Right to Vote*. Ithaca, NY, USA: Cornell Univ. Press, 2012.

since this and other defamation decisions have been reached.

When I was at the Lindell Cyber Symposium, I listened to talks from people who convinced me that they were con men, pushing narratives that I am convinced they did not actually believe, but I also heard talks from people who I am convinced honestly believed that they had found evidence of fraud. When I looked at their evidence, I saw other (and to me, more plausible) explanations, but I cannot hold them guilty of defamation for reaching the conclusions they did.

Convictions can deter con men and hucksters, but how can they deter honest people who reach incorrect conclusions? And, of course, there are innocent people who want to believe that the election was stolen, and both accept and act on what they learn from people they consider to be experts.

It's also important to remember that election denial is not partisan and does not require either slander or defamation. After the Florida recounts of 2000, some blamed that debacle on defective punched cards sold by Sequoia Voting Systems.[7] While some conspiracy theories attributed this to malice on the part of Sequoia, Roy Saltman's analysis of Florida 2000 uncovered what amounts to a comedy of errors, most of which were accidents—and the most ethically questionable of which had nothing to do with punched cards.[8] Some of the conspiracy theories being promulgated by today's stop-the-steal movement have their origins in the Ohio 2004 presidential race, notably theories about votes being sent across political boundaries so outside actors could alter them.[9]

BERGHEL: *Forbes* reported that Smartmatic settled its claim against One America News Network for an undisclosed amount on 16 April 2024.[10] However, this still leaves an impressive number of related lawsuits open, including Smartmatics' US$2.7 billion suit against Fox,[11] as well as personal suits against Fox News anchors Lou Dobbs and Maria Bartiromo, Trump attorneys Rudy Giuliani and Sidney Powell, and alleged election conspiracy theorists Mike Lindell and Patrick Byrne, to name but a few. In your opinion, what is the end state of all of these prosecutions?

JONES: I think that there is strong merit to many of the cases, but I expect many of the plaintiffs to lose. The reason is that news anchors, attorneys, and salesmen can easily claim that they were relying on expert opinions. If the defendants can convince the courts that they honestly believed those experts and that they were not aware of any credible challenges to the credibility of their experts, then they are likely to walk free.

Convictions can deter con men and hucksters, but how can they deter honest people who reach incorrect conclusions?

BERGHEL: Amid the election denialism following the 2020 presidential election, Mike Lindell's Cyber Symposium advertised convincing proof that the election was stolen. You mentioned previously that the symposium fell way short of its advertised claims. Have there been any new and related developments since that symposium?

JONES: I have not seen significant changes in the conspiracy theories. What has emerged is a sense of orthodox doctrine so that people who express doubt that the election was stolen are subject to excommunication. With this orthodoxy, there's been a decrease in the detail of the conspiracy theories I've seen. Now, it seems sufficient for loyal conspiracy theorists to proclaim that the election was stolen—without presenting any particular detail.

BERGHEL: Much has been made of the ease with which one may use generative artificial intelligence (AI) tools to create misinformation. To what extent do you feel that this might impact future elections?

JONES: Generative AI makes it cheaper to produce convincing forgeries, but it doesn't really change the nature of forgery. Stalin didn't need generative AI to erase political opponents from photographs of historical events. Moon-landing denialists didn't need generative AI to claim that the moon landings were a hoax created by Hollywood special effects.

What generative AI does is reduce the price of forgery. Photoshop makes it fairly easy to delete people from photos using its content-aware fill tool. Generative AI tools allow even more. We've already seen AI used to create convincing robocalls from candidates to mislead voters.[12] While such fakes are illegal, I imagine that we'll be seeing more of this, particularly in the form of doctored photos and videos circulated on social media.

Even without AI, parody has a long history of being mistaken for reality. *The Onion*, for example, has run many satirical stories that readers mistook for news.[13] The problem has become serious enough that it has a name, *Poe's Law*: It is impossible to write a parody that someone will not mistake for the genuine article unless it is clearly marked as such.[14] Unfortunately, Internet trolls know this and dodge responsibility for deeply offensive material by claiming that the material is merely parody and that those who are offended are victims of Poe's Law.

Bogus campaign claims have been around since the dawn of politics. Candidates have long misrepresented the positions of their opponents. We have

reached the point where we expect Republicans to call New Deal Democrats communists, and we expect Democrats to call main-street Republicans fascists. Selective quotations, sound bites, and video clips can paint a candidate as far more extreme than they really are. Misquoting a candidate to make them sound more extreme than they are is also common, if unethical. Using a deep fake to alter a sound bite or video clip is comparable to a deliberate misquote.

> Generative AI makes it cheaper to produce convincing forgeries, but it doesn't really change the nature of forgery.

Unlike a misquote, deep fakes cannot be accidental; if a campaign uses one, it must be considered malicious.

Deep fakes have serious potential as a legitimate form of political parody. Instead of having an actor parody a politician, why not use AI to create a deep fake of that politician doing exactly what the actor might have portrayed? Bernie Sanders said of Larry David's parodies, "He does a better Bernie Sanders than I do."[15] Would it be worse to use deep fake technology to create such parodies? I don't think so, but it is a short step from parody to political misinformation and slander. All it takes is a failure to clearly mark the content as parody and Poe's Law will come into play.

BERGHEL: In your book with Barbara Simons,[16] you quoted a former Chicago ward alderman who said that Chicago's switch to voting machines led many precinct captains to subscribe to *Popular Mechanics*. Can a similar case be made for present-day political operators subscribing to *Wired* and *Ars Technica* for the latest trends in AI?

JONES: That quotation had a tongue-in-cheek element. *Popular Mechanics* does not teach how to pick locks or rig mechanical voting machines. *Wired* and *Ars Technica* do not teach how to rig e-voting systems. But, as Charles Babbage noted in 1832, while beautiful inventions are rare, both technical skill and inventiveness are fairly common.[17] As new technologies are developed, large numbers of people will eventually learn to use them, and the unscrupulous among them will abuse them.

It's interesting to try to estimate the population of programmers competent enough to be serious security threats. If we assume that programmers have a 40-year working life, and we assume two big universities in each of the 50 states, each turning out 50 programmers per year, that comes to 200,000 people. Assume that 99% are honest, and you have a population of 2,000 people who pose a serious threat.

I pulled those numbers out of thin air, but the point is, it's wrong to rely on the obscurity of our technology as a defense. In the days of hand-counted paper ballots, our adversaries understood what could be done with pen, pencil, and paper. In the days of mechanical voting machines, our adversaries understood what could be done with rubber bands, bits of pencil lead, cigarette lighters, lock picks, and other mechanical tools. Today, we should expect our adversaries to understand cryptography, digital signatures, injection attacks, and self-replicating code.

BERGHEL: What is the state-of-the-art in voting machine technology in 2024? How reliable are voting machines now, compared to 2022 when we last addressed this issue?

JONES: Voting technology did not change much in two years. The fraction of voters using hand-marked paper ballots is almost unchanged. The fraction using direct-recording electronic voting machines has fallen from 6.7 to 5%, with a corresponding increase in the use of electronic ballot-marking devices.[18]

In November 2023, there was a noteworthy ballot-marking device failure in Northampton County, PA, USA. In a judicial retention race, some voters who selected YES on the screen had paper ballots printed that said NO and vice versa. The cause was a clerical error made by the voting system vendor in their role as a contractor to the county for the job of configuring the machines. The error should have been detected in preelection testing, but the vendor also acted as a contractor in designing the preelection tests that failed to detect the error.[19] Sadly, the potential for such an error had been clearly described three years previously.[20]

Many election jurisdictions outsource much of the work involved in managing election technology to voting machine vendors and election service companies. While large urban jurisdictions can easily afford to retain in-house technical staff to do this work, small jurisdictions have little choice but to hire contractors. For more than 20 years, I have argued that small jurisdictions should be able to pool their resources to afford appropriately trained election staff, but such arrangements are very rare.

For several years, there have been proposals to use advanced cryptography to secure elections. Many of the early proposals rested on the use of cryptography to secure end-to-end guarantees for paper-based elections.[21] More recently, there have been widely criticized proposals—and even commercial products—using blockchain technology for voting over the Internet.[22] Military and expat voters have been asking for some way to use modern technology to vote for several decades. This pressure will continue; the problem remains an open research area.

BERGHEL: From the point of view of accuracy, integrity, security, and the protection of voter privacy, how do things stand with state voting registration databases? How well are they currently audited?

JONES: Voter registration databases in the United States are inherently difficult to maintain. Unlike most European countries, the United States does not have a national database of citizens. Voter registration databases are maintained by the states. ERIC, the Electronic Registration Information Center, has long helped states recognize duplicate voter registrations. Such duplication is quite common because when people move between states, they frequently forget to cancel their old registration.

One of the core myths of the stop-the-steal movement has been that huge numbers of votes were cast illegally by dead people and by people registered to vote in multiple states. The first conspiracy theories about ERIC date to 2016, and they emerged again in 2022. In 2023, these conspiracy theories led a number of states to pull out of ERIC.[23] This significantly weakened ERIC and left the departing states scrambling for alternative ways to check their voter registration databases.[24]

With ERIC weakened and a number of states scrambling for alternatives, an organization called *True the Vote* released an app designed to crowdsource the task of cleaning voter registration rolls. This app, called IV3, helps users identify voter registration records they wish to challenge. The result has been a flood of voter registration challenges at already underresourced local election offices around the United States.[25]

BERGHEL: *The Washington Post* reports that the State of Arizona is training election workers to spot AI-based deep fakery that might be used to subvert election integrity by fooling election workers with spoofed communications from election officials.[26] It seems to me that such training is critically needed for both election workers and the general public—and not just to train election workers to spot fake communications but for the electorate to spot bogus campaign claims. Your thoughts?

JONES: Indeed. Deep fakery has the potential to make spear-phishing attacks far more difficult to distinguish from legitimate communications. In the past, creating an effective spear-phishing attack required labor-intensive research into the target. Deep fakery has the potential to greatly reduce this cost. This is not a new threat. All of us should already be deeply suspicious of phone calls and e-mails involving security-critical subjects.

Early this year, many New Hampshire voters received misleading robocalls delivering a deep-faked message from President Biden. The message was quickly tracked to a Texas-based robocall contractor, and the AI software used to create it was identified.[27] I expect we'll be seeing significantly more of this.

Databases of personal information allow targeting advertising at carefully selected segments of the population. Over the past decade, political campaigns have made extensive use of this to target precisely crafted advertising to voters.[28] Candidates have always crafted their message to their audience: for example, giving a different speech to a union meeting than they give to a chamber of commerce luncheon. Nevertheless, the resemblance between the fine-grained narrowcasting that is now possible and spear phishing is significant. I expect that we will soon see similar narrowcasting of deep fakes, with material carefully crafted to mislead particular demographics.

To return to the Arizona example, I do not see how a "curriculum" to train people to recognize deep fakes could possibly work. The technology is evolving rapidly enough that the "tells" that worked last week are unlikely to work next week.

BERGHEL: You and Barbara Simons begin your seminal 2012 book[16] on election integrity with the following 1934 quote from Joseph Harris:[29]

> "There is probably no other phase of public administration in the United States which is so badly managed as the conduct of elections."

It is now nearly a century after Harris wrote his book on election administration. How far have we come in addressing his concerns?

> Today, we should expect our adversaries to understand cryptography, digital signatures, injection attacks, and self-replicating code.

JONES: We have made progress since then, but there is considerable room for improvement. The U.S. Election Assistance Commission adopted version 2.0 of the Voluntary Voting Systems Guidelines in early 2021.[30] These guidelines are nominally voluntary, but a sufficient number of states require compliance that they effectively set the standard to which voting equipment is built. Version 2.0 is a significant improvement over its predecessors, but it suffers from significant shortcomings. Section 301(a)(5) of the Help America Vote Act of 2002 creates one of these limitations by narrowly defining voting system accuracy to exclude errors "attributable to an act of the voter."[31] Unfortunately, this exclusion means that the voting system standards cannot regulate a central feature of any voting machine: how accurately it captures the voter's intended votes.

California has been doing post-election ballot tabulation audits since 1965, but for many years, they were alone. After the 2000 presidential election, more states have joined. Today, 35 states have mandatory post-election audits, and an additional eight have discretionary audits. Of the 35 with mandatory audits, six states have statistically strong risk-limiting audits.[32]

Unfortunately, many of the states have mandatory audits that are weak. A very common failing is to tell the auditors the expected tally before the audit and then let them count and recount until they "get it right." Even with such weaknesses, audits have routinely found and corrected numerous problems.

Ballot tabulation audits are effective only if the ballots subjected to audit are the ballots actually cast by the voters. If the chain of custody from polling place to audit is weak, then no matter how statistically sophisticated the audit, it will produce only weak results. Twenty years ago, I pointed out that jurisdictions can take some very simple auditing measures, such as comparing the number of ballots issued to voters with the number of ballots cast and comparing that with the sum of all votes in vote-for-one races.[33] There is obviously a problem if the sum of the votes exceeds the number of ballots or if the number of ballots exceeds the number of voters. Unfortunately, many states release only the vote totals for each candidate, preventing the public from performing these elementary checks.

Although Article I, Section 4 of the U.S. Constitution permits Congress to regulate the place, time, and manner of elections, Congress has largely left these issues to the states.[34] This is why our national voting system standards are officially guidelines. The lack of uniformity in state voting rules has a significant cost. Consider a simple issue: the order in which the candidates for office are listed. Some states protect the ruling party by listing candidates in order by the fraction of the vote their party took in the most recent statewide election. Others rotate the candidates so that each candidate is listed on top on an approximately equal number of ballots, but there seem to be almost as many rotation rules as there are states that rotate. A voting system vendor interested in a national market must support all of these options. Furthermore, when voting systems are approved for use in a state, it is because, in principle, the system can be configured correctly for that state. It is up to the end user, the local election administrator, to make sure that each of the configuration options is set correctly.

> In the long run, improved accuracy and integrity earn public confidence, but these goals can conflict in the short run.

Finally, there is tension between two obvious goals for election administrators. One goal is to maintain or increase public confidence in our system of elections. The stop-the-steal movement is clear evidence of a decline in public confidence, and this must be reversed. Another goal is to maintain or improve the accuracy and integrity of our election system. In the long run, improved accuracy and integrity earn public confidence, but these goals can conflict in the short run.

U.S. elections are massive undertakings, frequently involving as much as 1% of the electorate in election administration. In any enterprise of that size, we should expect problems. When audits and transparency expose problems, this can reduce public confidence. One way to increase confidence is through public relations (PR) campaigns. I am worried that too many election officials have responded to the stop-the-steal campaign with PR campaigns and not with measures that actually earn confidence.

REFERENCES

1. A. Feuer and M. Escobar, "The Jan. 6 Riot inquiry so far: Three years, hundreds of prison sentences," *The New York Times*, Jan. 2024. Accessed: Jul. 1, 2024. [Online]. Available: https://www.nytimes.com/interactive/2024/01/04/us/january-6-capitol-trump-investigation.html
2. T. Dresbach and N. Caldwell, "The Trump campaign embraces Jan. 6 rioters with money and pardon promises," *NPR*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.npr.org/2024/01/04/1218672628
3. Z. Petrizzo. "Lindell-apalooza melts down." Salon. Accessed: Jul. 1, 2024. [Online]. Available: https://www.salon.com/2021/08/12/lindell-apalooza-melts-down-mypillow-guy-claims-antifa-sabotaged-his-cyber-symposium/
4. K. Himmelman, "The big reveal that wasn't," *The Dispatch*. Accessed: Jul. 1, 2024. [Online]. Available: https://thedispatch.com/article/the-big-reveal-that-wasnt/
5. L. Hagen, "The ReAwaken America Tour unites conservative Christians and conspiracy theorists," *NPR*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.npr.org/2022/11/02/1133477897
6. N. Narea and A. Prokop, "Fox pays $787 million for its 2020 election lies," *Vox*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.vox.com/politics/2023/4/18/23688613/fox-dominion-settlement-trial-2020
7. K. Zetter, "Sequoia voting systems responsible for 2000 presidential debacle?" *Wired*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.wired.com/2007/08/sequoia-voting/
8. R. Saltman, *The History and Politics of Voting Technology*. New York, NY, USA: Palgrave MacMillan, 2006.
9. K. Zetter, "Did Ohio election data run through republican servers?" *Wired*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.wired.com/2007/04/did-ohio-electi/
10. A. Durkes, "Smartmatic settles OANN defamation case: Here's where dominion and Smartmatic's other lawsuits stand now," *Forbes*.

Accessed: Jul. 1, 2024. [Online]. Available: https://www.forbes.com/sites/alisondurkee/2024/04/16/smartmatic-settles-oann-defamation-case-heres-where-dominion-and-smartmatics-other-lawsuits-stand-now/?sh=772b50f8639a
11. E. Pilkington, "Fox News braces for more turbulence as second defamation lawsuit advances," *The Guardian*, Mar, 2023. Accessed: Jul. 1, 2024 [Online]. Available: https://www.theguardian.com/media/2023/mar/13/smartmatic-defamation-lawsuit-against-fox-news
12. S. Bond, "A political consultant faces charges and fines for Biden deepfake robocalls," *NPR*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.npr.org/2024/05/23/nx-s1-4977582
13. K. LaCapria. "Were hundreds of Cuban refugees clinging to air force one on flight back to US?" Snopes. Accessed: Jul. 1, 2024. [Online]. Available: https://www.snopes.com/fact-check/cuban-refugees-clinging-to-air-force-one/
14. E. G. Ellis, "Can't take a joke? That's just Poe's law," *Wired*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.wired.com/2017/06/poes-law-troll-cultures-central-rule/
15. A. Feldman, "Actually, it would be big news if Bernie sanders and Larry David weren't cousins," *The Forward*, Oct. 2017. [Online]. Available: https://forward.com/fast-forward/384378/
16. D. Jones and B. Simons, *Broken Ballots: Will Your Vote Count?* Stanford, CA, USA: CSLI Publications, 2012.
17. C. Babbage, *On the Economy of Machiery and Manufactures, Paragraph 313*. London, U.K.: Charles Knight, 1832.
18. "The verifier—Election day equipment, 2022 and 2024." Verified Voting. Accessed: Jul. 1, 2024. [Online]. Available: https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024
19. K. Skoglund. "Election problems in Northampton county, PA in November 2023, citizens for better elections." Securiosa. Accessed: Jul. 1, 2024. [Online]. Available: https://securiosa.com/posts/northampton_problems_2023.html
20. A. Appel, R. DeMilo, and P. Stark, "Ballot marking devices (BMDs) cannot assure the will of the voters," *Election Law J.*, vol. 19, p. 3, Sep. 2020.
21. D. Chaum et al., "Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes," in *Proc. USENIX/ACCURATE Electron. Voting Workshop*, San Jose, CA, USA, Jul. 2008. [Online]. Available: https://www.usenix.org/legacy/event/evt08/tech/full_papers/chaum/chaum_html/index.html
22. S. Park, M. Specter, N. Narula, and R. Rivest, "Going from bad to worse: From Internet voting to blockchain voting," *Cybersecurity*, vol. 7, pp. 1, 2021. [Online]. Available: https://academic.oup.com/cybersecurity/article/7/1/tyaa025/6137886
23. M. Parks, "How the far right tore apart one of the best tools to fight voter fraud," *NPR*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.npr.org/2023/06/04/1171159008
24. M. Parks, "Republican states swore off a voting tool. Now they're scrambling to recreate it," *NPR*. [Online]. Available: https://www.npr.org/2023/10/20/1207142433
25. D. Mehrotra, "Inside the 'election integrity' app built to purge US voter rolls," *Wired*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.wired.com/story/true-the-vote-iv3-app-voter-fraud/
26. S. Ellison and Y. Sanchez, "In Arizona, election workers trained with Deepfakes to prepare for 2024," *The Washington Post*, May 2024. Accessed: Jul. 1, 2024. [Online]. Available: https://www.washingtonpost.com/politics/2024/05/08/arizona-election-workers-trained-with-deepfakes-prepare-2024/
27. K. Manson, "How investigators solved the Biden Deepfake Robocall mystery," *Bloomberg*. Accessed: Jul. 1, 2024. [Online]. Available: https://www.bloomberg.com/news/newsletters/2024-02-07/how-investigators-solved-the-biden-deepfake-robocall-mystery
28. N. Singer, "This ad's for you (not your neighbor)," *New York Times*, Sep. 2022. Accessed: Jul. 1, 2024. [Online]. Available: https://www.nytimes.com/2022/09/15/business/custom-political-ads.html
29. J. Harris, *Election Administration in the United States*. Washington, DC, USA: Brookings, 1934.
30. "Voluntary Voting System Guidelines." U.S. Election Assistance Commission. [Online]. Available: https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines
31. "One Hundred Seventh Congress of the United States of America." U.S. Election Assistance Commission. Accessed: Jul. 1, 2024. [Online]. Available: https://www.eac.gov/sites/default/files/eac_assets/1/6/HAVA41.PDF
32. "The verifier—Post election audits." Verified Voting. [Online]. Available: https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/audit/year/2024
33. D. W. Jones. "Auditing elections." *Commun. ACM*, vol. 47, no. 10, pp. 46–50, Oct. 2004.
34. "Constitution of the United States." U.S. Senate. 00MC00-microelectronics-3437828: [Online]. Available: https://constitution.congress.gov/constitution/
35. H. Berghel, "The state of the art in voting machine technology: Just how reliable are they?" *Computer*, vol. 55, no. 1, pp. 18–126, Jan. 2022, doi: 10.1109/MC.2021.3126494.

HAL BERGHEL is a professor of computer science at the University of Nevada, Las Vegas, Las Vegas, NV 89154 USA. Contact him at hlb@computer.org.