

Point/Counterpoint

The U.S. Should Ban Paperless Electronic Voting Machines

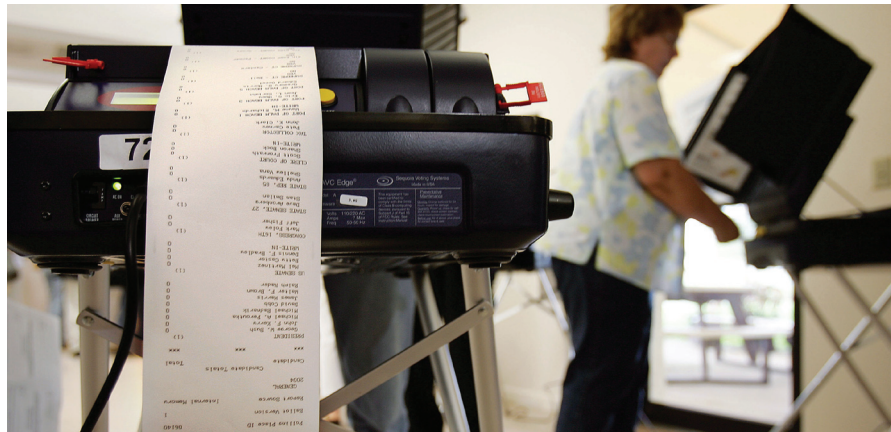
Debating the public policy issues involved in proposed efforts toward improving voting systems while considering the range of technical and societal challenges.

Point: David L. Dill

WHEN U.S. VOTERS go the polls next month, it will be impossible to determine whether the victorious candidates in many states were elected by a software bug, a virus in the voting system, the voting system programmers, or the voters themselves. Those states have voting machines that rely entirely on electronic ballots (these machines are referred to as direct-recording electronic voting machines, or DREs). There is no way to tell whether the votes recorded by DRE machines match those selected by the voters.

The solution is straightforward: Ban the use of untrustworthy paperless DREs, and demand that readily available systems that are auditable, accurate, reliable, accessible, and cost-effective be used in their place.

Paperless electronic voting is unworkable in principle with current technology. It is based on the mistaken idea that we can build computers that can be trusted to carry out operations whose results cannot be independently verified. But that's a practically impossible problem to solve, even given our best efforts. There is no way to know whether any of the many people involved in the design, implementation, and manufacture of the machines made a mistake or introduced a malicious change. If that were to happen, enough votes could be corrupted to



change the outcomes of many elections—invisibly. This fact raises questions about all elections utilizing paperless DREs. Even if the machines are counting votes perfectly, we have no way of confirming that.

Why are paperless DREs more risky than the computers we rely on for banking, medical equipment, and flight software? It's because there is independent verification of the results of operating these other systems. If your plane lands in the wrong city or crashes, or your pacemaker malfunctions, either you or your survivors know about it. If banking software makes an error, you can check your statements to find it. But paperless DREs have no independent verification. If votes are changed in a plausible way, how will anyone ever know?

In reality, current DREs are not even close to “best efforts,” as has been shown repeatedly, especially in the last

year. Security reviews in California^a and more recently in Ohio^b documented breathtaking blunders in the security designs of the most widely used DRE systems in the U.S, which collectively process millions of votes. In each case, a single person with limited access could introduce a virus into the system during one election that could take over all the voting systems in the jurisdiction in the next election.^c

It is urgently necessary to ban cur-

a M. Bishop, “Overview of Red Team Reports,” Top-to-Bottom Review, California Secretary of State's Office; www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf.

b A press release on the EVEREST study of voting equipment security for the Ohio Secretary of State is available at www.sos.state.oh.us/SOS/PressReleases/2007. Detailed reports are available at www.sos.state.oh.us/SOS/elections/voterInformation/equipment/.

c There is a video of team at Princeton showing several ways to hack the Diebold AccuVote-TS DRE at youtube.com/watch?v=aZws98jw67g.

rent paperless DREs. Many states have already done so, but many states have not. All voters who go to the polls in Maryland and Georgia are forced to use paperless DREs, as are many voters in other states. Some other states are using paper ballots now, but could decide to convert to paperless e-voting in the future. Without federal legislation, voters in some states will be stuck with DREs for a long time.

Congress should mandate a specific class of paper trails: every voter should mark and cast a voter-verified paper ballot (VVPB). Each ballot can be counted by hand or scanned in the precincts by a scanner that checks it for overvotes or stray marks (the technical term for this type of system is precinct-count optical scan or PCOS). If there is a problem, the voter has a chance to fix the ballot or fill out a new one. Otherwise, the ballot is counted and deposited in secure ballot box. Or ballots can be counted by hand if desired. These systems can be made accessible to voters with a wide range of disabilities through the use of ballot-marking devices, which allow paper ballots to be read, marked, and verified via an accessible electronic interface.

Most studies have shown that PCOS systems are at least as accurate as any other voting system. They are less costly than touchscreen machines, and, if they fail, marked ballots can be stored in a ballot box and counted later. Most importantly, the hand-marked ballots can be verified and counted without having to trust computerized systems. Optical scan systems are already the dominant technology in the U.S.—they have been used for many years and the

Some have argued that legislation requiring paper ballots would hamper innovation in voting technology. But the main problem in voting technology is not a lack of innovation, but how to prevent and recover from bad innovations.

technology is steadily improving.

Why paper and not some other permanent medium such as recordable compact discs? Paper can be read and written by people or machines, and, importantly, by (almost) everyone without machine assistance. Votes on paper cannot be removed or changed without detection. Critical documents on paper have been handled for many centuries and the procedures are easily understood by poll workers and election administrators. For example, it is easily recognized as a problem if a poll worker disappears into a back room for a few hours with a box of ballots.

Of course, simply using paper ballots does not guarantee election in-

tegrity. The ballots must be protected, and the processes for storing, transporting, handling, and counting them must be transparent. Crucially, paper ballots enable the routine auditing of elections by choosing ballots from randomly selected precincts or machines and manually counting them to see if they match the machine totals.

Some have argued that legislation requiring paper ballots would hamper innovation in voting technology. But the main problem in voting technology is not a lack of innovation, but how to prevent and recover from bad innovations. State and local governments chose to purchase tens of thousands of DREs in spite of the dire warnings of computer technologists and activists—then the true risks of DREs turned out to be even worse than the warnings. The existing requirements and certification process did little to protect the voting system from this and other bad ideas.

A federal VVPB mandate would channel vendor R&D efforts into improving optical scan technology, instead of developing and marketing lucrative but ultimately dubious systems like DREs. If and when a radically new technology is proposed, the law can be changed—after a thorough debate about the true benefits, costs, and risks of that new technology—a debate that would have averted the disastrous experiment with DREs over the last few years. **C**

David L. Dill (dill@cs.stanford.edu) is a professor of computer science and electrical engineering at Stanford University and has been working actively on policy issues in voting technology since 2003.

Counterpoint: Daniel Castro

ALL VOTERS WANT and deserve secure elections; unfortunately, no voting system currently on the market offers voters verifiable proof that their ballot has been counted. Some activists have been especially concerned about the integrity of votes cast on direct recording electronic (DRE) voting systems, since these devices rely on software that can be difficult to au-

dit. While most individuals agree that voting technology should be improved, many people disagree on the best way to improve it. In particular, a vocal group of activists have popularized the idea of using paper audit trails—basically a paper receipt produced by the DRE—as a countermeasure to fraud and error. Unfortunately, this proposal is an incomplete solution to a much larger problem. Moreover, improving voting systems is not merely a technical challenge but also a public policy challenge.

Computer science is an academic discipline that is based in logic and proof, and we should rely on these valuable methods in our analysis of voting system technology. To understand the scope of the problem one must first understand that the voting process does not end at the ballot box; to have secure elections every step of the voting process must be secure. Specifically, ballots must be cast as intended, collected as cast, and counted as collected. Paper audit trails only provide verification of

the first step—that the ballot was cast as intended. That’s good, but not good enough. It does not matter to voters if the voting system correctly cast their ballots, if they cannot verify that election officials correctly counted them.

In fact, narrowly focusing on paper trails ignores the importance of securing all steps in the voting process. Improving election security will involve improving multiple security controls including software testing, physical security, parallel testing, and pre- and post-election auditing. Moreover, paper audit trails are not the only option to verify that ballots are cast as intended. Many types of audit trails will suffice, including those that use audio and video. For example, a research team at Auburn University has developed the Prime III voting system, which produces a private, independent, voter-verified video audit trail of the on-screen interactions between the voter and the voting system.

Additionally, an entirely new class of voting systems has been designed by cryptographers that offer end-to-end (E2E) verifiability of all three steps of the voting process. These E2E systems give voters a paradoxical combination of proof and privacy—proof their ballot is included in the final vote tally and privacy to prevent vote selling and voter coercion. Examples of E2E voting systems include PunchScan (see www.punchscan.org), VoteHere (www.votehere.com/vhti.php), and Scratch & Vote.¹ (In addition, see the news story “Clean Elections” on page 16. —Ed.)

Unfortunately, many of these considerations have been absent from the debate, which has narrowly focused on whether or not to require paper audit trails rather than the larger question of how to improve voting systems. In order to provide a convincing answer to this question security experts and election officials must develop a quantifiable risk analysis framework for evaluating and comparing risk in voting systems. In addition, they must conduct a cost-benefit analysis of the proposed policies for improving voting systems. These two initiatives will provide the evidence and knowledge base on which to base any decisions on proposed design changes to voting systems. Most debate on voting system improvements is premature given that security experts and elections officials have not yet developed a com-

prehensive risk analysis to compare voting systems. To skip these steps is not only bad science, but bad policy.

The crucial first step to improving voting systems is for the Election Assistance Commission—the federal commission charged with improving elections—to conduct a rigorous and methodical risk assessment of each class of voting system (such as DRE, optical scan, and lever). To date, there has been no comprehensive risk assessment of this type that would allow a meaningful comparison of the relative risks of different voting systems. No voting system is perfect, but as with any system, the key is to find an acceptable level of risk. In addition, a risk assessment would give policymakers a realistic picture of the differences in security between different voting systems. A number of projects have laid the foundation for such a framework, including the NIST’s *Developing an Analysis of Threats to Voting Systems*³ and the Brennan Center report *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*.²

The second step for improving voting systems is to conduct a cost-benefit analysis of proposed voting system improvements. A cost-benefit analysis would reveal the hidden impact of these

Mandating paper audit trails could preclude any chance of implementing these systems in the near future. Rather than turn back the clock on voting technology, we should develop policies that encourage innovation in our voting systems.



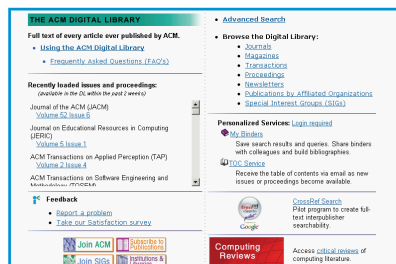
proposals on security, usability, accessibility, and cost. For example, paper audit trails reduce some risks from software threats but introduce new risks from the chain-of-custody of the paper trails. In addition, paper audit trails decrease accessibility, as blind voters are unable to independently verify the paper audit trail. Paper audit trails are also expensive—in addition to the cost of printers, counties must pay to securely collect, transfer, track, store, and count the paper trails.

While voting system security receives a lot of attention, it is only one of many requirements that voting systems must satisfy. For example, a completely secure voting system is worthless if it is so complex that nobody can use it. Similarly, voters will reject an extremely user-friendly voting system if it is not secure. In voting systems, as with any other type of system, competing values should be balanced against each other. Only with both a risk assessment and a cost-benefit analysis in hand can policymakers implement those design changes that offer the best overall improvements in security, usability, accessibility, and cost.

Finally, security experts and election

ACM Digital Library

www.acm.org/dl



The Ultimate Online INFORMATION TECHNOLOGY Resource!

- **NEW! Author Profile Pages**
- **Improved Search Capabilities**
- **Over 40 ACM publications, plus conference proceedings**
- **50+ years of archives**
- **Advanced searching capabilities**
- **Over 2 million pages of downloadable text**

Plus over one million
bibliographic citations are
available in the ACM Guide
to Computing Literature

To join ACM and/or subscribe to
the Digital Library, contact ACM:

Phone: 1.800.342.6626 (U.S. & Canada)

+1.212.626.0500 (Global)

Fax: +1.212.944.1318

Hours: 8:30 a.m. – 4:30 p.m., EST

Email: acmhelp@acm.org

Join URL: www.acm.org/joinacm

Mail: ACM Member Services

General Post Office


PO Box 30777

New York, NY 10087-0777 USA

officials must recognize that improving voting systems is not a short-term project. Most of the substantive improvements in voting systems will likely not come from short-term patches, but through long-term technical innovation. In particular, cryptography and E2E voting systems offer potential for revolutionizing voting. Yet mandating paper audit trails could preclude any chance of implementing these systems in the near future. Rather than turn back the clock on voting technology, we should develop policies that encourage innovation in our voting systems. To begin, federal funding needs to be available to sponsor voting system research and development, pilot testing, and risk assessment evaluations.

In addition, voting system guidelines should define functional standards (such as requiring independent, voter-verifiable audit trails), rather than technologically restrictive design standards (such as paper audit trails). Functional standards define the minimum operational requirements to which a system must conform. Since functional standards do not define any specific technology or process, they are flexible enough to allow researchers to develop new approaches to solve existing problems. Just as government should not require that all computers run Windows, neither should it require that all voting machines use paper.

Policymakers cannot disregard voting system technology, and computer scientists cannot ignore the public

policy implications of their recommendations. The real challenge is not to design the perfect voting machine, but to design the perfect election. This question is neither exclusively in the domain of computer science nor exclusively in the domain of public policy. Instead, experts from many fields must work together to develop a solution that satisfies all of the characteristics of a good election. While quick-fix ideas may sound good on paper, a deeper analysis shows that many of these proposals suffer serious faults. Moreover, paper trails are not a short-term solution to security, as they only address a small portion of a larger problem. Reinforcing the front door of a house is pointless if the back door is wide open. Instead of trying to apply an unproven and expensive paper patch to existing voting systems, security experts and policymakers should lay out a strategy to advance voting system technology based on a reasoned analysis and solid evidence. 

References

1. Adida, B. and Rivest, R.L. Scratch & vote: Self-contained paper-based cryptographic voting. In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society (WPES'06) (Alexandria, VA, Oct. 30, 2006), ACM, NY, 29–40.
2. Norden, L. et al. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*. Technical report, Brennan Center for Justice at NYU School of Law, October 2006.
3. The National Institute of Standards and Technology. *Developing an Analysis of Threats to Voting Systems*; vote.nist.gov/threats/.

Daniel Castro (dcastro@itif.org) is a senior analyst at the Information Technology and Innovation Foundation (www.itif.org) a non-profit, non-partisan public policy organization in Washington, D.C.

Rebuttal: David L. Dill

I HAVE ARGUED that the U.S. voting system is in crisis due to the ill-advised adoption of inherently flawed DRE (direct-recording electronic) voting machines, which are opaque and highly insecure against attacks by both insiders and outsiders. Fortunately, this problem can be easily solved by using voter-marked ballots and precinct-count optical scan technology (PCOS), which is already in widespread use and has proven to be reliable and cost-effective. In particular, I do not argue

for adding printers to DREs—PCOS is the best option for voter verification of ballots.

Daniel Castro says a paper trail will not solve all problems in voting. That's true, and no surprise to advocates of paper ballots. Paper ballots are an essential ingredient in a trustworthy election system, which must also include rigorous physical security of ballots, manual counts to audit election results, and other procedural and legal safeguards. But trustworthy elections are impossible with current paperless DREs. The manufacturers and programmers of

the machines, and even external attackers with no special access, can completely control the storage and counting of votes.^a

Castro says the focus on paper trails ignores other aspects of voting systems. In reality, advocates of PCOS systems have thought through the broader issues, including cost, accuracy, and accessibility. In all these dimensions, PCOS systems are competitive with DRE systems.

Castro argues we cannot act without a “quantifiable risk analysis framework,” and a “cost-benefit analysis.” Risk analysis and cost-benefit analysis are great ideas; DREs would never have been purchased had these types of analyses been performed and heeded.

a M. Bishop, “Overview of Red Team Reports,” Top-to-Bottom Review, California Secretary of State’s Office; www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf.

However, legislation need not wait for further study because DRE systems are clearly much riskier than PCOS systems, a fact that demands prompt action. The most comprehensive study so far (which is the basis for a summary cited by Castro) concludes that a single individual could alter the outcome of a close election on paperless DREs, but that a much larger team of attackers would be required to steal an election using PCOS—assuming appropriate procedures including manual audits.^b As for cost-benefit analysis, PCOS systems obtain the benefits of DREs and more, at lower cost.^c

b Norden, L. et al. *The Machinery of Democracy: Protecting Elections in an Electronic World*. Brennan Center for Justice at NYU School of Law, October 2006 (see p. 50 and p. 83); brennan.3cdn.net/52dbde32526fdc06db_4sm6b3kip.pdf.

c See www.verifiedvotingfoundation.org/article.php?list=type&type=77.

Castro claims there are other ways of solving the problems of electronic voting, including the Prime III system and several end-to-end systems (Punchscan, VoteHere, and Scratch&Vote). Prime III has video and audio (rather than paper trails) that would be very difficult to audit in practice. Punchscan and Scratch&Vote are arguably voter-verified paper ballot systems, albeit cryptographic ones. More importantly, these systems will not be available to replace DREs for years (if ever). VoteHere’s system, which also had paper receipts, never caught on, possibly because election officials, technical reviewers, and the public found it difficult to understand.

It is unacceptable in a democracy to have election results that could be undetectably tainted by bugs or malicious software. There is no excuse for further delay in implementing a readily available solution to this serious problem. ■

Rebuttal: Daniel Castro

WHILE DAVID DILL makes a passionate case for paper ballots, he omits one stubborn fact: historically, paper ballots are at the root of most voting fraud. This is not surprising since paper ballots can be easily changed, lost, stolen, or invalidated. Yet his solution is to throw more money at precinct-count optical scan (PCOS) systems. While these paper-based voting machines have some initial appeal, they are not a panacea.

First, his claim that PCOS systems are less costly than other forms of voting technology is simply false. This is akin to claiming that apples are more expensive than oranges. The total cost of a voting system for a county depends on many factors: the price and quantity of the voting devices, the number of elections per year, the lifecycle of the equipment, and the cost of recounts, storage, maintenance, and disposal.² Moreover, any proposal to change voting technology must also take into account the cost of switching technology, such as retraining election officials.

Second, PCOS systems can be hacked. In fact, the Brennan Center writes in its report on voting systems, “Nothing in our research or analysis has shown that a Trojan horse or other software attack program would be more difficult against PCOS systems than they are against DREs.”¹ Manual recounts prevent some attacks, but not all of them. For example, an attacker could disable the over/under-vote alert on the optical scanners in certain counties resulting in many invalid ballots. Since over/under-votes account for up to 4% of total votes, this attack could swing a close election.

Moreover, PCOS systems do not provide voters any proof their ballots were included in the final tally. Neither do PCOS systems offer any kind of guarantee to voters that no illegitimate ballots have been added to the tallies. The only way to achieve that level of confidence is to provide end-to-end (E2E) verifiability, which is why I recommend E2E voting systems as a long-term solution.

As a short-term solution, we should tighten up security requirements to eliminate known vulnerabilities and ensure consistent election procedures.

Election officials can use pre- and post-election auditing to make sure the machine does what it is supposed to do, parallel testing to make sure it works correctly during the election, and hash-code testing to make sure the software that is on the machine is the same software that was previously tested and is on file.

States can make their current e-voting systems reasonably secure without a federal requirement for paper audit trails. Switching every county to PCOS or paper ballots would cost over \$1.1 billion, and still not solve the security problem. And ultimately, switching to PCOS or paper ballots is a waste of time, money, and effort because it does not move us to where we want to go: end-to-end verifiability. Requiring paper ballots will only move us sideways or even backward—we should move forward. ■

References

1. Norden, L. et al. *The Machinery of Democracy: Protecting Elections in an Electronic World*. Brennan Center for Justice at NYU School of Law, October 2006.
2. Norden, L. et al. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*. Technical report, Brennan Center for Justice at NYU School of Law, October 2006.