Handout: The truth about our computerized election systems

By Jennifer Cohn
Protect Our Votes
February 16, 2018

Our elections are under attack. Intelligence officials concur that Russia plans to target the 2018 midterm elections.[1] One hundred experts in the fields of computer science and statistics have recommended paper ballots and post-election statistical audits to protect our democracy.[2] But some election officials have undermined efforts to implement these security measures with irresponsible and false assurances that it would be difficult for hackers to alter the outcome of a national election under our current system.[3]

This handout strives to break through this disinformation with sourced facts that expose the truth about our computerized voting systems. We hope that concerned citizens will use this handout as a tool to persuade decision-makers of the urgent need for paper ballots, robust post-election audits, and other security measures.

The truth about our computerized election systems

As computer science professor Alex Halderman explained during a congressional briefing in July 2017, "[H]acking a national election in the United States would be, well, shockingly easy."[4] Here are the facts:

All voting machines are at risk of internet hacking, even if they are not directly connected to it. "Over 9,000 jurisdictions (counties and states) in the U.S. run elections with a variety of voting machines: optical scanners for paper ballots, and direct-recording 'touchscreen' machines."[5] Contrary to popular belief, all such voting machines can be hacked through the internet, even if they are not directly connected to it.[6] Before every election, all voting machines must accept programming to reflect the races on the ballot. They receive this programming via memory cards from computers that are themselves often connected to the internet.[7] All precinct results are sent to central tabulators, often via vulnerable local networks.[8] And central tabulators then

transmit results to *online* Election Night Reporting Systems, providing easy access for internet hacking.[9]

Corrupt insiders with direct access are also a major threat. Electronic tallies can also be altered by *corrupt insiders* with direct access to the voting machines or memory cards.[10] Computer Science professor Andrew Appel (Princeton) has shown that it takes only a screwdriver and about seven minutes to install a vote-stealing program into a DRE. [11] As for optical scanners, they use memory cards that can be programmed without detection to add, subtract, or shift as many votes as a rigger chooses.[12] At the 2017 Def Con Hacking Conference, "every piece of equipment in the Voting Village was effectively breached in some manner. Participants with … only limited tools and resources were quite capable of undermining the confidentiality, integrity and availability of these systems."[13]

Systems are not decentralized. The claim that voting systems are "decentralized" is often used to provide reassurance that widespread, systemic meddling is not possible. However, just two voting machine vendors account for more than 80 percent of U.S. voting equipment.[14] And the computers used to program the voting machines before each election are themselves centralized at the state or county level.[15] In some states, a single third-party vendor may perform the programming for most or all voting machines in the state.[16]

While paper ballots can be used to verify the legitimacy of electronic tallies, fourteen states use paperless machines. The only way to verify whether an election has been hacked is to compare the electronic tally to the paper ballots.[17] While electronic tallies from optical scanners can be verified (because optical scanners count paper ballots), tallies from paperless DREs are unverifiable. The following five states exclusively use such paperless machines: Georgia, New Jersey, Louisiana, South Carolina, and Delaware.[18] Another nine states—including the swing states of Florida and Pennsylvania—include at least some counties with paperless machines.[19] After the 2016 election, the state of Virginia made the decision to discard their DREs in favor of paper ballots.[20]

DREs with Voter Verified Paper Audit Trails ("VVPATs") are bad too. DREs with VVPATs—voting machine printouts that are supposed to reflect voter intent— are almost as bad as paperless machines. Studies show that voters rarely review the difficult-to-read VVPATs for accuracy, and don't notice computer vote flips even when they do.[21] It has proven difficult or impossible to manually count or audit VVPATs.[22] And hackers have repeatedly shown that the printed result can match the voter's choices, while the internal memory records whatever choice the hacker wishes it to record.[23] DREs were initially promoted as a means to accommodate voters with disabilities, but states bought them for *all* voters regardless of need, creating a 15 year election-integrity crisis.[24] Disability groups have since called for their elimination.[25]

Ballot Marking Devices ("BMDs") are poised to follow in the dangerous path of DREs. BMDs are assistive "electronic pencils" that generate *computer*-marked paper

ballots, which are then counted on optical scanners like hand-marked ballots. As with DREs, voters may never actually review the ballots for accuracy. BMDs have been promoted for voters who are unable to hand mark ballots. But some states plan to buy them for *all* voters, regardless of need,[26] adding an unnecessary extra layer of vulnerable electronics to our already vulnerable elections.

States rarely conduct manual recounts, even in close elections. Paper ballots make hand recounts possible, but states rarely allow them.[27] Most require a hand recount, if at all, only when the margin of victory is less than a small percent.[28] From a rigger's standpoint, this simply serves as an invitation to shift enough votes to exceed the recount margin. As we saw in 2016, courts rarely allow a meaningful hand recount when that margin is exceeded.[29] The cost for elective recounts, where allowed, is often prohibitive.

Manual audit laws are absent and/or inadequate. States could address the manual recount problem by enacting laws requiring statistically meaningful manual audits after *every election*, with full hand recounts in the rare situations where audit results warrant them. But experts have determined that only a few states conduct audits that are anywhere close to sufficient to detect electronic tampering.[30]

Some election officials destroy ballot images. Most optical scanners used today produce digital images of the ballots as they count them.[31] These images are public records, but some election officials destroy them.[32]

Vendors are not transparent. Most voters are unaware that taxpayer money goes to election equipment vendors with close past and/or present ties to such eyebrow-raising individuals and entities as: a foreign dictator thought to have rigged his own election, a sophisticated cyber-felon, U.S. politicians, and the far-right Council for National Policy.[33] These vendors use the proprietary nature of their code and hardware to successfully block forensic examinations of their taxpayer-funded systems.[34] Thus, no memory card in any U.S. election has ever been subject to inspection for hacking or malicious programming.

Emergency security protocols for 2018 and beyond

Hand-marked paper ballots. The United States ambassador to the United Nations, Nikki Haley, recently told the Democratic Republic of Congo not to use electronic voting:

> "*These elections must be held by paper ballots so there is no question by the Congolese people about the results. The U.S. has no appetite to support an electronic voting system*."[35]

Americans also deserve trustworthy elections. Thus, hand marked paper ballots must be available to all voters in time for the 2018 midterm elections, with assistive devices provided for those who are unable to hand mark their ballots.

A return to paper ballots means replacing DREs with optical scanners or hand counting. Jurisdictions may claim they can't afford new scanners to count the paper ballots. If so, point out that some counties in Virginia *leased* scanners to ensure the integrity of Virginia's last election.[36] Other jurisdictions can do the same.

If states still refuse to buy or lease optical scanners, then demand that they publicly hand count the paper ballots instead. This is not asking too much. *Spurred by serious concerns about transparency and security, most Western democracies—including Germany, France, Canada (for federal elections), Norway, and the Netherlands—have rejected voting machines in favor of publicly hand-counted elections*.[37] Although U.S. ballots tend to be more complex than in countries that hand count, most county election boards already have emergency hand-count protocols that can be implemented. Manual counting, *if completed on Election Night*, would not present the chain-of-custody problems that arise when we rely on next-day, or even-longer-delayed, manual audits to ensure the integrity of computerized election systems.

Many counties in New Hampshire already conduct publicly hand-counted elections as a matter of course. According to the manual linked here,[38] the ballots include on average 15 races and yet are fully hand counted within several hours on Election Night.

Risk limiting audits ("RLAs") or modified full hand-count audits. RLA's or modified full hand-count audits must be mandated for every race in 2018.

RLA's are a type of statistical audit endorsed by Verified Voting, Common Cause, the League of Women Voters, the American Statistical Association, and others.[39] Full hand-count audits are a kind of RLA where ballots are run through optical scanners and then hand counted under bi- or multi-partisan supervision.[40] A modified full hand-count audit—the type of audit already conducted in Columbia County, New York--is the same as a full hand-count audit, but it excludes uncontested races and it hand counts fewer ballots in races with very large victory margins.

All audits must be open to the media and the public. Elections must not be certified until the auditing process is complete and the audit results have either confirmed the accuracy of the initial vote count or led to a full manual count (the results of which will be dispositive).

The chain of custody must be transparent and demonstrably secure. Post-election audits and recounts depend on a demonstrably secure *chain of custody* between Election Night and the audit (or recount), the period in which the public loses sight of the ballots.[41] The chain of custody procedures must also be *transparent* or public confidence in the audit result will falter. During the 2004 presidential recount, ballots were "marked or altered, apparently to ensure that the hand recount would equal the machine count."[42] And in 2016, paper ballots were destroyed before they could be

recounted in the Wasserman-Schultz/Canova U.S. House race.[43] This can't happen ever again in any election.

Ballot images must be preserved. States must also follow federal law and protect election transparency by preserving ballot images as public records.[44]

Precinct results must be posted. Where precinct counting is done, precincts must post results to the public before transmitting them to the tabulators. This transparency measure would allow citizens to detect and deter any tampering or error that might occur after the results leave the precincts.

Vendor transparency. To provide a measure of transparency, election equipment and software vendors and contractors must publicly (a) disclose the names of each of their officers, directors, and owners; (b) disclose the names of each of their parent companies, as well as the parent companies' respective officers, directors, and owners; and (c) warrant that no one affiliated with the company or with a parent company (as officer, director, owner, employee, contractor, or consultant) has been convicted of a felony.

Advocating for change

Please contact your members of Congress and ask them to support the bipartisan federal Secure Elections Act, which would allocate federal funds for states to replace DREs with paper ballots and optical scanners. The Act, however, is not a panacea, as states would retain the right to decide whether and when to use these federal funds. Moreover, the Act would require statistical audits only for federal elections and not until 2022. Conditions and circumstances are such that this delay is unacceptable.

Thus, in addition to supporting the Act, please demand action from your state legislators and state and county Election Boards. If states can't or won't buy or lease optical scanners in time for the 2018 midterms, then they should conduct precinct-based hand counts, looking to New Hampshire for guidance. Consider sending them copies of one or more of the following documents in support of these demands:

- **This handout.**

- **The September 2016 report of Computer Science Professor Andrew Appel,** which recommended both paper ballots and statistical manual audits. https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Appel-Princeton-Testimony.pdf

- **The November 2017 written congressional testimony of Professor Matt Blaze (University of Pennsylvania)**, which also recommended both paper ballots and statistical "risk limiting" audits for every race. https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf

- **The letter from 100 experts calling for paper ballots and statistical risk limiting audits in federal elections.** This document addressed only federal elections because it was drafted in anticipation of the federal Secure Elections Act, but the same reasoning and urgency applies to state and local races and referendums. https://www.electiondefense.org/election-integrity-expert-letter/

- **The report from the 2017 Def Con Hacking Village Conference**. https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

- **Academic report titled "Evidence-based Elections"** by Professor of Statistics Philip B. Stark (U.C. Berkeley) and Professor of Electrical Engineering David A. Wagner (U.C. Berkeley) re: the need for paper ballots, risk limiting audits, and a secure chain of custody between Election Night and the audit. https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

- **The Bush Center report on election security**, including recommendation for paper ballots. http://www.bushcenter.org/publications/articles/2018/01/we-should-be-hardening-our-defenses.html

Additional Resources

Secure Our Vote has organized a grass roots campaign to lobby state and local election boards for paper ballots and Risk Limiting Audits. Their website also has excellent written training materials.[45]

Verified Voting has a terrific website.[46] Its "Verifier" tool shows the type of voting equipment used in each state. Verified Voting also has a state audit law database.

Citizens for Election Integrity Minnesota has an excellent website where you can search for each state's recount and audit laws.[47]

Center for American Progress posted an extremely helpful report grading each state on its voting and registration system security as of February 12, 2018.[48]

Bio and Acknowledgements

Background: Jennifer Cohn is an attorney and election integrity advocate in the San Francisco Bay Area who graduated from UCLA and Hastings College of the Law. As an attorney, her areas of practice included insurance coverage and appellate law. She practiced law for more than twenty years, including seven years as a partner with Nielsen Haley & Abbott, LLP in Marin County, California. Since 2016, she has devoted her professional efforts full time toward investigating our insecure election system and potential solutions. She can be contacted through her Twitter account, @jennycohn1.

Acknowledgements: Thank you to election integrity advocates **Jonathan Simon** (author of *Code Red, Computerized Election Theft and The New American Century* and blogger at CodeRed2014.com/blog*),* **Brad Friedman** (host of the *BradCast with Brad Friedman* radio show and a blogger at bradblog.com), **Lulu Friesdat** (Emmy Award winning journalist and documentarian), and **Philip B. Stark** (Professor of Statistics at U.C. Berkeley) for their substantial time and effort helping produce this handout.

End Notes

[1] https://www.washingtontimes.com/news/2018/feb/13/russia-plans-2018-midterm-elections-interference-i/?utm_campaign=shareaholic&utm_medium=twitter&utm_source=socialnetwork

[2] https://www.electiondefense.org/election-integrity-expert-letter/ [letter from 100 experts];

See also https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Appel-Princeton-Testimony.pdf [Professor Appel congressional testimony, 9/28/16];

https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf [Professor Blaze congressional testimony, 11/29/17]

[3] https://www.c-span.org/video/?c4668571/alex-halderman-voting-system [C-span interview of EAC Commissioner Thomas Hicks and Computer Science Professor Alex Halderman, via Marilyn Marks]

[4] https://www.youtube.com/watch?v=AD3qqBfU0no [video of Computer Science Professor Alex Halderman's July 2017 Congressional debriefing; Halderman is a "professor of computer Science and Engineering at the University of Michigan" and is "part of a small community of computer experts who have spent the better part of the last ten years focused on the security of our election machinery."]

[5] [1b]https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/ [Article by IT Professor Andrew Appel: "Which voting machines can be hacked through the internet? …The answer: all of them."]

[6] Ibid.

[7] https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/ … [Article by IT Professor Andrew Appel: "Which voting machines can be hacked through the internet? …The answer: all of them."];

https://thinkprogress.org/how-easy-would-it-be-to-rig-the-next-election-819326cbbbd/ … [Professor Dan Wallach, manager of Rice University's Computer Security Lab, agrees that "When you dig down, [many vendors] often have election management systems connected to the Internet, albeit behind firewalls, VPNs, or other such devices. It's incorrect to call such systems 'never connected.'"]

https://www.youtube.com/watch?v=AD3qqBfU0no [video of Computer Science Professor Alex Halderman's July 2017 Congressional debriefing: "Somehow, before the election, the machines have to receive their programming: who's on the ballot. And this comes from a computer called an Election Management System. Often, these Election Management System computers are connected to the internet. And if the Election Management System computer is targeted by attackers and infected, that infection can spread to the memory cards that are going to program all of the voting machines in that entire area."]

[8] https://d3n8a8pro7vhmx.cloudfront.net/jillstein/pages/26798/attachments/original/1480973902/Wisconsin_Hursti_Affidavit_11-28-16_(00268311x9CCC2).pdf?1480973902 …

[9] https://www.scmagazine.com/researchers-fear-georgia-special-election-still-vulnerable/article/668925/
["While Merle King, Executive Director of CES, claims that the election system is 'air-gapped,' he fails to disclose that the system, including vote tabulation databases, is exposed to cyber attack through counties' repeated use of the same flash drive to move election night tabulation interim iterations to the election night reporting application on the web."]

[10] https://www.salon.com/2015/04/15/the_great_american_voting_scam_how_political_insiders_are_gaining_the_power_to_steal_our_elections/ ["The greater threat to most systems comes not from external hackers, but from insiders who have direct access to the machines," the report noted. "There is no reason to trust insiders in the election industry any more than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it."]

https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Appel-Princeton-Testimony.pdf [Professor Appel congressional testimony, 9/28/16]

[11] https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144

[12] https://www.eac.gov/assets/1/28/EVEREST.pdf, pp. 137–38 [describing how optical scanner memory cards can be hacked]

https://www.dailykos.com/stories/2005/6/1/118600/- …[describing Harri Hursti hacking demonstration of optical scanner memory cards]

https://whowhatwhy.org/2016/10/31/easy-hack-voting-machines-endanger-democracy/

[13] https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf [Report from Def Con Hacking Village]

[14] https://trustthevote.org/wp-content/uploads/2017/03/2017-whartonoset_industryreport.pdf, p. 28 [Election Systems & Software and Dominion Voting account for 81% of U.S. voting equipment; Hart Intercivic accounts for another 11%]

[15] https://www.c-span.org/video/?c4668571/alex-halderman-voting-system [IT Professor Halderman: "[E]ven though voting machines themselves are not connected to the internet, the voting machines have to receive the data about the ballot design and about the software that's running on them from somewhere. And they get that data from **central** systems in the counties or states. These are called Election Management Systems."]

[16] https://wcmcoop.com/2012/05/22/meet-command-central-the-people-in-charge-of-wisconsin-voting-machines/; ["Command Central," a two-person company, does all election system programming for Wisconsin]

https://www.motherjones.com/media/2005/11/recounting-ohio/ [Triad responsible for programming tabulators in 41 Ohio counties]

[17] https://medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba ["Want to know if an election was hacked? Look at the ballots"]

[18] https://www.salon.com/2017/05/16/as-millions-pour-into-georgias-congressional-runoff-the-voting-machinery-is-among-the-worst-in-america-hackable-paperless-unverifiable_partner/ [article re: states that use paperless machines]

[19] Id.

[20] https://www.washingtonpost.com/local/virginia-politics/virginia-scraps-touch-screen-voting-machines-as-election-for-governor-looms/2017/09/08/e266ead6-94fe-11e7-89fa-bb822a46da5b_story.html?utm_term=.2d03185d51c0

[21] https://medium.com/@jennycohn1/ballot-marking-devices-add-a-second-layer-of-vulnerable-electronics-to-our-elections-5f6bcfe82adb [Sourced article re: VVPATs and Ballot Marking Devices]

[22] Id. See also http://www.bradblog.com/?p=4682 ["Study: Two-Thirds of Voters Fail to Notice Vote-Flipping on Touch-screen DRE Voting Systems"]

http://www.wheresthepaper.org/Tobi_PaperBallotElecAdminBasics_July19_07.pdf ["Election Science Institute Study of DRE VVPAT for Cuyahoga County showed a ten percent error rate for VVPAT printouts, rendering these votes unreadable and unusable for hand counts in an audit or recount situation."]

https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf ["Voter marked paper ballots are the best form of VVPR. Thermal paper print of the kind typically generated by direct-recording electronic voting machines (DREs) is particularly fragile and subject to spoilage."]

https://arstechnica.com/information-technology/2007/04/congress-finally-considers-aggressive-e-voting-overhaul/ ["Serious concerns were raised regarding the flaws with the printers used to produce paper audit trails. Norris cited a Las Vegas survey in which fewer than 40 percent of voters actually checked the paper record of their vote before leaving the polling place. An election official in North Carolina reported that there were hundreds of printer failures in that state during the 2006 election. He cited a Georgia

study about the logistical challenges of storing, tracking, and manually counting thousands of votes recorded on unwieldy rolls of paper tape."]

[23] https://d3n8a8pro7vhmx.cloudfront.net/jillstein/pages/26798/attachments/original/1480973902/Wisconsin_Hursti_Affidavit_11-28-16_(00268311x9CCC2).pdf?1480973902 …

[24] https://www.wired.com/2004/10/diebold-and-the-disabled/ ["In the controversy over electronic voting machines, activists for disability groups have been at the forefront of campaigns to convince counties and states to purchase touch-screen voting systems."]

https://www.eff.org/wp/accessibility-and-auditability-electronic-voting

https://www.wired.com/2003/11/dust-up-over-e-vote-paper-trail/ ["The California Association of Clerks and Election Officials, or CACEO, led by Shasta County Clerk Ann Reed, called the decision [to require a paper audit trail] "a major defeat for the disabled community, as well as the minority-language communities."];

http://www.baltimoresun.com/news/maryland/bal-md.machines29mar29-story.html ["Advocates for visually impaired voters are concerned that the paper trail requirement will strip them of their right to a secret ballot…"]

https://books.google.com/books?id=XR21acqXy28C&pg=PA161&lpg=PA161&dq=DREs+blind+touchscreens&source=bl&ots=bKjbw2-0WK&sig=T0sJRg83H-oaAPsNJ1tMozcKjkw&hl=en&sa=X&ved=0ahUKEwib0dWa54_ZAhWl7YMKHZZcAEUQ6AEIVjAJ#v=onepage&q=DREs%20blind%20touchscreens&f=false , p. 161

https://www.pbs.org/newshour/politics/should-primary-voters-be-worried-about-aging-voting-machines [initially, 70% of the machines bought under HAVA were DREs]

[25] http://electiondefensealliance.org/2007/03/disability_voter_advocates_call_ban_dres ["BLIND AND DISABLED VOTER ADVOCATES, GROUPS CALL FOR 'IMMEDIATE BAN' OF DRE VOTING SYSTEMS!"]

[26] https://www.wabe.org/ga-lawmakers-look-new-voting-machines-cost-big-unknown/ [Georgia looking into BMD's];

http://www.latimes.com/local/lanow/la-me-ln-county-voting-system-20160630-snap-story.html ["Touchscreen ballots … could be the future of voting in L.A. County."]

[27] https://medium.com/@jennycohn1/it-is-difficult-to-get-a-hand-recount-in-the-u-s-even-when-voting-machines-use-paper-ballots-3a9b65feea60;

See also http://ceimn.org/ceimn-state-recount-laws-searchable-database/states/Michigan [state recount law and state audit law databases]

[28] Id.

[29] https://medium.com/@jennycohn1/it-is-difficult-to-get-a-hand-recount-in-the-u-s-even-when-voting-machines-use-paper-ballots-3a9b65feea60

[30] Id.

[31] https://www.youtube.com/watch?v=5wrxNYaFOvA&feature=youtu.be [John Brakey video—Ballot images create a paradigm shift in verifying elections]

http://blackboxvoting.org/ballot-images/

[32] https://columbusfreepress.com/article/did-gop-strip-flip-2016-selection [Husted in Ohio allows election workers to turn off ballot image audit function]

https://whowhatwhy.org/2017/12/11/voters-left-dark-alabamas-election-system/ [Merrill in Alabama allows election officials to turn off ballot image "save" function]

https://www.aspentimes.com/news/marks-prevails-in-jefferson-county-case/

https://arizonadailyindependent.com/2017/05/31/pima-county-judge-rules-in-favor-of-voter-privacy-ballot-images-same-as-ballots/ [court treats ballot images as public records]

[33] https://medium.com/@jennycohn1/updated-attachment-states-have-bought-voting-machines-from-vendors-controlled-and-funded-by-nation-6597e4dd3e70 [article compiling sources re: disturbing voting machine vendor ownership and connections]

[34] https://www.pbs.org/newshour/science/heres-how-hackers-could-mess-with-electronic-voting ["Plus, much of this voting technology is proprietary, so forensic auditors couldn't independently scrub for and detect malicious software, especially given such code might delete itself after Election Day, Scott said."]

https://www.thenation.com/article/touch-and-go-elections-perils-electronic-voting/ ["[T]he public can't examine the very software they use to vote. In fact, such scrutiny is illegal. The voting software that runs on the electronic machines is considered 'proprietary information' by the companies that produce it, therefore no one, not even election officials, can access it."]

http://www.bradblog.com/?p=8986 ["Auditing the operation of this code is difficult because the formats of the flash cards [which hold voter selections recorded by the iVotronic machines] and of Unity's internal database are both proprietary," Eckhardt explains in his report. "[S]ince no one of them can be audited without access to proprietary data, the behaviors of the three bodies of code, as a group, cannot readily be audited."]

[35] https://www.reuters.com/article/us-congo-politics-un/u-s-warns-congo-against-electronic-voting-for-delayed-election-idUSKBN1FW24U?il=0

[36] http://wavy.com/2017/11/07/paper-ballots-make-a-return-across-virginia/ [some Virginia counties leased scanners]

[37] http://www.dw.com/en/german-election-volunteers-organize-the-voting-and-count-the-ballots/a-40562388 [Germany]

https://digitalcommons.wcupa.edu/cgi/viewcontent.cgi?referer=https://t.co/rFYaJOq2QP&httpsredir=1&article=1002&context=crimjust_facpub [Canada]

https://www.pcworld.com/article/3178417/security/fears-of-election-hacking-spread-in-europe.html [France]

https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html [The Netherlands]

https://thebarentsobserver.com/en/life-and-public/2017/09/norwegian-votes-be-counted-manually-fear-election-hacking [Norway]

https://medium.com/@jennycohn1/breaking-news-most-western-democracies-flee-voting-machines-america-clings-to-them-while-refusing-569e5036695f [compilation of sources re: countries that hand count their elections]

[38] http://www.wheresthepaper.org/Tobi_PaperBallotElecAdminBasics_July19_07.pdf [Election Defense Alliance Manual re: Hand Counted Paper Ballots—New Hampshire counties as an example]

[39] https://www.verifiedvoting.org/resources/post-election-audits/ ["The risk limiting audit is the gold standard of audits"; [In 2010, "the American Statistical Association issued a statement endorsing risk-limiting post-election audits."];

https://www.stat.berkeley.edu/~stark/Seminars/penn11.pdf, p. 3 [Risk Limiting Audits are endorsed by Common Cause, the American Statistical Association, the League of Women Voters, and others].

For more information about RLAs, please contact computer scientist *Barbara Simons* and U.C. Berkeley Professor of Statistics Philip B. Stark.
https://www.verifiedvoting.org/resources/post-election-audits/

https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf

[40] For more information about full hand count audits, please contact Virginia Martin, Commissioner on the Columbia County, New York, Board of Elections.

https://countedascast.files.wordpress.com/2017/10/2-tier-approach-to-audits-oct-2017-friesdat.pdf [article by election integrity advocate Lulu Friesdat describing full hand count audits conducted in Columbia County, New York; includes comments by Virginia Martin, commissioner on the Columbia County Board of Elections].

https://www.csmonitor.com/USA/Politics/2017/1107/Securing-the-vote-How-paper-can-protect-US-elections-from-foreign-invaders [article re: full hand count audits including comments by Virginia Martin]

https://www.youtube.com/watch?v=nh3nSTonD3g [Virginia Martin presentation to the California Election Integrity Coalition re: full hand count audits]

[41] https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf, p. 3 [Academic report re: the importance of "compliance audits" to maintain a secure chain of custody between Election Night and any post-election audit]

[42] http://www.motherjones.com/media/2005/11/recounting-ohio/# …

[43]http://www.hollerbackfilm.com/blog/canova-ws-ballots-destroyed

[44] http://blackboxvoting.org/the-brakey-method/ ["A Colorado citizen named Marilyn Marks filed, and won, a succession of lawsuits establishing that both ballots and ballot images must be treated as public records in Colorado."]

https://arizonadailyindependent.com/2017/05/31/pima-county-judge-rules-in-favor-of-voter-privacy-ballot-images-same-as-ballots/

For more information about ballot images, please contact *John Brakey* of Audit AZ and *Bev Harris*, author of *Black Box Voting: Ballot Tampering in the 21st Century*.

[45] https://secureourvote.us/take-action/

[46] https://www.verifiedvoting.org/

[47] http://ceimn.org/ceimn-state-recount-laws-searchable-database/states/Michigan [state recount law and state audit law databases]

[48]

https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/ [discusses and "grades" each state's election equipment, voter registration equipment, and auditing laws]