

Is Auditing an RCV Election Possible?

Dick Atlee, 19 January 2016

On the surface, a hand-count audit of a random sample of a large (e.g., Maine's 700K ballots) Ranked Choice Voting (RCV) election seems conceptually impossible, since the result is dependent on taking all ballots into account. The question is, is there some less direct yet feasible and dependable approach that could accomplish the same goal.

Here are two possibilities (there may be more):

1. One, devised by me in consultation with an RCV proponent, involves comparing a hand count of random local jurisdictions with both the original results from those jurisdictions and the results from reruns on the machines that originally tabulated them (to deter "Volkswagen" test trickery).
2. The other, based on work done by software developer Mitch Trachtenberg in Humboldt County, CA, involves no randomness, but rather machines and handwork -- the independent re-scanning of ballots and their conversion to public spreadsheet data for transparent "hand" calculation of the results.

I'll outline both here. However, it is important to keep in mind that neither procedure will be in effect if/when RCV is passed in November. And unfortunately, the changes in laws, rules, procedures and equipment required to bring these about are not the kind of gut-level no-brainer issue that has brought RCV so far. Thus, they seem far less likely to ever be implemented, particularly in an environment of the denial of the existence of election theft. ***Without them -- or some equivalent audit method -- RCV leaves us with impossible-to-verify elections.***

Both approaches need to be viewed in the Maine environment of about 500 municipalities, in which half tabulate 80% of the vote on optical scanners, and half (smaller communities) hand-count 20% of the vote.

Audit Method #1: Random Subsets With an Open Source RCV Algorithm

I've heard various estimates of what percentage of the vote from randomly selected sites is necessary to effectively detect election theft -- from 1-2% to 5% and up. I've also heard from on-the-ground people that such percentages are the creations of academics who have no grasp of a hard reality -- i.e., that "random" can be and is defined and interpreted to suit particular interests, and thus is not a useful auditing concept. However, this first auditing method assumes that some percentage and randomization scheme can be determined that works and is practically implementable. To the extent that randomization is not trustworthy, Audit Method #2 would be preferable.

1. RCV election summary:
 - a. Scanner memory cards are sent to a central location
 - b. Hand-count ballots are sent to be scanned either to this location or regional centers.
 - c. Final results are produced by an algorithm. The requirements for this to be auditable are:

1. The software that implements the algorithm must be open source, AND
2. The totals for each of the rank-order permutations must be available in publicly accessible records
3. The first part of the audit is a **scanner integrity check**
 - a. The scanners to be checked are:
 1. A random selection of scanner jurisdictions, AND
 2. The central scanner for hand-count jurisdictions, using ballots from a random but discrete set of jurisdictions -- or, if regional scanning is done, then each regional scanner scans ballots from a random set of jurisdictions within that region.
 - b. Method used (will also detect the "Volkswagen" test-vs-vote hack):
 1. Rerun the ballots from that jurisdiction through the scanner
 2. Hand count those ballots
 3. Compare these two results with the actual election results from that scanner
4. The second part is an **algorithm integrity check**
 - a. Use the ballots used in the scanner-integrity checks (they're now a known quantity)
 - b. Run them through the algorithm
 - c. Hand "count" them to get the permutations
 - d. Manually run these through the RCV process
 - e. Compare the manual- and algorithm-produced results.
5. If the both the scanner and the algorithm integrity tests check out, there is a high probability that the election was not tampered with.

Standard caveat: If all of these procedures are not implemented in law and rules, there would be no effective protection against sophisticated election theft.

Audit Method #2: Independent Same-Day Re-Scan/Tabulation

Carolyn Crnich, a forward looking election registrar (<https://vimeo.com/39740758>) in Humboldt County, CA, responded to the concerns of two commercial fishermen about the non-transparency of the optically scanned vote in the county. From this developed the Humboldt Transparency Project, in which software developer Mitch Trachtenberg (<http://www.mitchtrachtenberg.com/>) developed the Transparent Election Verification System (<http://player.vimeo.com/video/35785956>). TEVS is open-source software (source code is online and free to download) that can scan ballots using an off-the-shelf scanner, extract the data from them, and put the data in a spreadsheet, from which simple procedures can be used to produce election results that can be checked against the official voting and RCV algorithm results. This would appear to be more simple and straightforward than Audit Method #1. It goes like this:

1. Each polling place (and the central or regional scanning locations) that is using a DS200 optical scanner is supplied with a separate, inexpensive off-the-shelf scanner (or more than one, proportional to the voting load); or it can use its own scanner.
2. After the election closes, the people who would normally be called upon to count the ballots instead shuffle them (to foil any preplanned fraud) and feed them through the scanner. This occurs at the rate of around 2000 ballots per hour, faster than most humans can operate.
[Note: election officials often say they have a hard time finding volunteers for counting or poll

work. One solution to this -- even for our current system -- would be to encourage the use high school community service time. But in any case, this audit method has less of a manpower/time requirement than the current system, thus minimizing late nights and human error.]

3. The scanned ballot images are digitally signed and sent to an independent organization -- or more than one such organization in order to increase credibility of the results. If there's any question about the accuracy of a given image, it has the serial number of the original ballot and can be compared.
4. The organization (or organizations) run the TEVS software on the ballot images to produce spreadsheets. In the case of an RCV race of N candidates, N columns of the spreadsheet -- one for each possible ranking -- would be assigned to each candidate. TEVS takes about 1 second per ballot on mid-range hardware.
5. For a plurality race, simply using the spreadsheet's SUM function is sufficient to determine all aspects of the race. For RCV races, the spreadsheet is sorted into the various permutations of rankings (i.e., for a 3-person race, the possible rankings are 123, 132, 213, 231, 312, 321). A simple manual RCV manipulation of these identifies the winner.
6. The spreadsheet and list of permutations are provided as public documents so that anyone can check them.

This is a totally transparent method for verifying the official results determined by non-transparent voting tabulation firmware/software. It solves the entire election integrity problem, regardless of whether RCV is passed or not. However, it has a number of pre-requisites:

1. Adapting the TEVS software (the source code is free, it currently runs under Linux) -- an easy project for a college computer science class.
2. Procurement of inexpensive scanners -- chicken-feed in terms of bang-for-buck, though money will be saved on the lack of licensing fees for the open-source software).
[Note: scanner procurement is optional -- a site can simply use its own scanner, in which case a Linux driver for such a scanner needs to be included in that site's TEVS implementation.]
3. Ballots must have serial numbers, which is also a protection against substitution of photo-copied ballots.
4. The law that holds that ballots or ballot images are *not* public records must be changed.
[Note: Given the importance of elections to the health of our democracy, why shouldn't they be public records? In the past, the greatest opposition to this policy has come from the voting machine companies, and you have to ask yourself, "Why?"]
5. The law stating that audits and recounts must be done by hand would not affect this, since this is not an official tally.

None of this is complicated, though -- regarding its chances of implementation -- the Humboldt County folks have found that most election officials outside their county are not sympathetic to proposals that change their usual way of doing business. RCV's proposal is doing just that, but it has a tidal wave of signatures and the coming vote riding behind it. Would RCV people also push for these minor changes? If they wouldn't, they've guaranteed non-transparent elections into the future.