October 2, 2020

A Hancock County Democrat

Not affiliated with or approved by the Hancock County Democratic Party

Election Insecurity

Bruce Workman

When you look at all of the factors affecting the accuracy and security of our elections, it comes down to the conflicts between protection against fraud, voter privacy, and transparency. It is important to remember that there are many different kinds of voting. Since voting rules and procedures are controlled by the states, there is the potential to have more than fifty distinct voting procedures. One method of voting is that done in the U.S. House of Representatives since the early 1970s. Members of Congress cast their votes with a specially designed machine and a large screen. When a representative inserts a special ID card, his or her name appears on the screen. The member then selects Yea, Nay, or Present, removes the card and the result appears next to the name. This is complete transparency. Everyone knows how everyone voted. It is not a secure method in the sense that it could be very easily hacked, but the transparency makes the hacking pointless. Any member could look at the screen and say "Hey, that's not how I voted."

Public elections in the U.S. operated much the same way until the late 1800s. Voting was done in public gatherings, usually featuring crowds of voters and onlookers. An election official would either call a voter's name or the voter would announce himself. The voter would announce his vote and another election official, or often the same one, would mark the vote on a chalkboard in the candidate's row or column to the cheers and jeers of the crowd. If we had this kind of transparency today, every voter could look on a spreadsheet to confirm his or her vote was correctly recorded. Cyber-tampering would be easily spotted, and results would be verifiable. By the late 1800s, vote-buying and coercion were rampant. For these tactics to work, verification is necessary. There is no point in buying a vote if one cannot know for whom or what the vote was cast. To stop candidates or committees from buying votes or intimidating voters, reformers urged the adoption of the secret ballot used in Australia. **(continued on page 2)**

Inside this issue:

Election Insecurity (continued from page 1)

By solving one problem others were created. The secret ballot has been used since its adoption in the 1890s. Now, the moment your vote is cast it loses any association with you and enters a stream of dissociated ballots. The dilemma created by open, public voting has been replaced with the lack of transparency. There is no longer certainty as to whether your vote was counted or whether it was counted correctly. The tradeoff of transparency for privacy has made it harder to detect ballot tampering and cast doubt on the legitimacy of our elections. The solutions that have been implemented have changed the nature of risk to voters. Election fraud has become rare, but ballots not being accepted or counted has become more prevalent. There is a much greater chance that your vote will not be counted that there is that your vote will be altered somehow.

There are three main suppliers of voting machines and software and since it is rather difficult to enter the field, they do not seem extremely interested in R&D or QA. County election officials are limited in their choices and experience frequent buyer remorse. One supplier (Diebold) famously left old source code on a public server in 2003. The sourc code was again leaked three weeks before the 2004 election. The solution they eventually came up with was to change the company name-sort of like putting lipstick on a pig. The most memorable malfunction in the election process is the infamous hanging chad affair in the 2000 election where officials were left to guess at voter intent.

In 1987, Yale University student and mathematician, Josh Benolah, submitted a doctoral thesis entitled “Verifiable Secret-Ballot Elections.” The gist of the paper was that new techniques in cryptology made it hypothetically possible to have an election in which everyone’s ballot could be kept secret and verifiable. For a more detailed explanation of what he was proposing, see the article “Lone Star” by Benjamin Wofford in Wired Issue 28.18. In the interim, I will attempt my simpler and less informed explanation in the following paragraphs.

Mathematicians had noticed something about the structure of RSA encryption. When text is digitalized it is translated as a series of 1s and 0s. When it is encrypted it is transformed into a large prime number called a ciphertext. What the mathematicians understood was when two ciphertexts were added or multiplied together, the mathematical relationship was maintained. In a simplified form, if one added the ciphertext for the number two to the ciphertext for the number four, the result would be the ciphertext for the number six. What this meant is that your votes could be encoded and still be countable and verifiable.

At a conference in 2011, Dana DeBeauvoir, Clerk of Travis County, Texas, decided to bury the hatchet in the ongoing war between election officials and academic critics, by announcing to the assembled scientists “…this country needs your wisdom, your knowledge of science and your help,” adding “Now is the time when you can put your mark on the future, and you can use Travis County to make that mark.” In the audience was Josh Benolah who began brainstorming on the spot. Also, in the audience was rice University commuter scientist Dan Wallach, a frequent critic of voting machines and a thorn in the side of election officials.

Benolah and Wallach teamed up with MIT’s Ron Rivest—the R in RSA—and STAR-Vote was born. STAR-Vote (secure, transparent, auditable, reliable) wanted to take the verification process further. Since the code was open source, a verification program could be written by anyone with coding skills to do so. Odds are that neither I nor anyone reading this would learn the protocols, but larger organizations, such as the League of Women Voters or one of the party National Committees could find the talent to do so. These organizations could then verify the elections and publish their results, thereby restoring trust in our elections. Even though the STAR-Vote created a final product, nobody could, or more correctly would build it. A report by the Wharton School of Business—yes, the same one Trump lied about attending—revealed that the business of election technology was an oligarchy of three vendors owned by private equity firms and were of low profitability and lacking funding to engage in any innovation. Unable to find anyone to build a machine, STAR-Vote died (kicking and screaming) in October 2017.

(contained on page 3)

Election Insecurity (continued from page 2)

Since 1997, Josh Benolah has worked as a computer scientist and cryptographer for Microsoft Corporation. Due to the relative size of the corporation and the election business, Microsoft had shown little interest in election machinery and software. The 2016 election changed that. In 2017, shortly after the death of STAR-Vote, Benolah received an email from someone high in the chain of command. Microsoft had begun searching for what it could do in elections that would not clash with its larger business interests. They asked Benolah if he could replicate what he had done, but this time for Microsoft. He readily agreed and in 2019 Microsoft launched Election Guard, which was based on the same encryption technology as STAR-Vote. They tried Election Guard in an election in Fulton, Wisconsin using paper ballots as a control. The results matched perfectly, and each voter could compare his or her encrypted receipt to the list to ensure the vote was counted. Election Guard will not be used in the 2020 election. "This is long-term for us, says Benolah. "If we get significant use in 2022, 2024, and beyond – we're happy." Maybe STAR-Vote was just ahead of its time.

The citizens of Fulton, a town in Rock County, Wisconsin, use the new system via VotingWorks machines for a Supreme Court candidate primary. However, the final vote was tallied via paper ballots, which were also printed after a user votes. To verify the reliability of Microsoft's software, paper ballots were checked against ElectionGuard results. **Photo courtesy of Microsoft Corporation**

Hancock County Democratic Party

Joe Biden for President

Nick Rubando for Congress

Melissa Kritzell for County Commissioner

Ohio Democratic Party

Democratic National Committee

Mobilize.us

Hancock County Board of Elections

October 5 is the deadline for Voter registration.

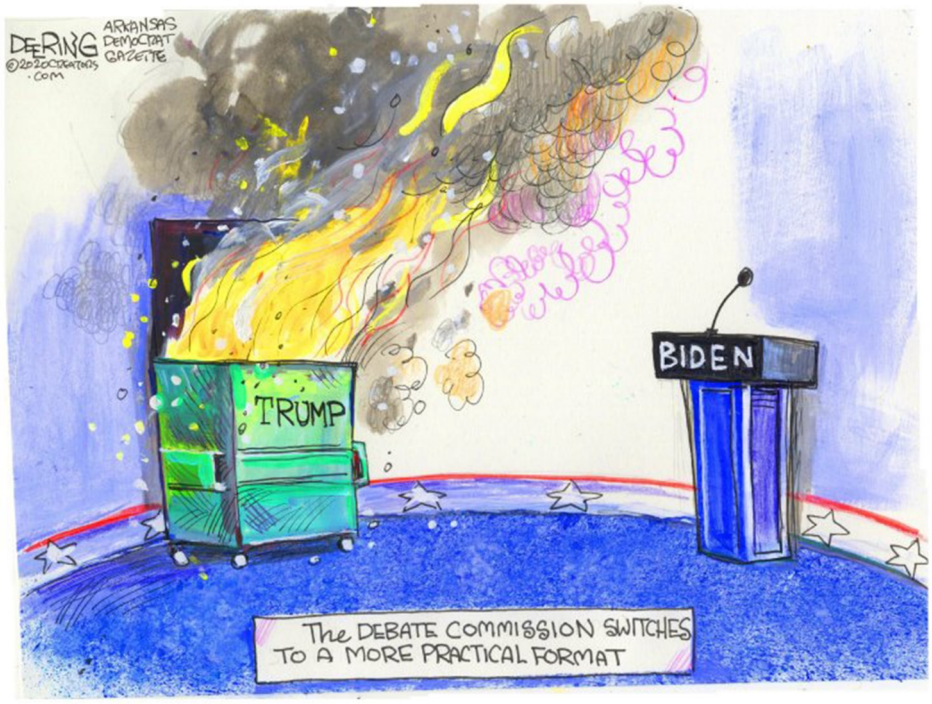
October 6 Absentee Ballots are ready for mailing.

October 6 Early Voting begins

32 Days to the General Election!

Saturday	**Pop-up booth w/Hancock County Young Democrats 10AM—1PM**
October 3, 2020	**Soul Squad Saturday with Sec. Julián Castro 3—4:30PM**
Sunday	**Brunch with Yang & the Gang: an Ohio Early Vote Kickoff 11—11:45AM**
October 4, 2020	
Monday	**Battleground OH: HOWA Monday Phonebank 5—7PM**
October 5, 2020	
Tuesday	
October 6, 2020	
Wednesday	**Ohio Day of Action Do-or-Dialer with new dialer training 5—8PM**
October 7, 2020	**KAMALA, CAKE and COCKTAILS*!! A Virtual Open House and Baking Competition (*mocktails welcome!) 7—9PM**
Thursday	**Pop-up booth w/Hancock County Democrats 4—6PM**
October 8, 2020	
Friday	
October 9, 2020	

JUST FOR FUN


DEERING
ARKANSAS DEMOCRAT GAZETTE
TRUMP
BIDEN
The DEBATE COMMISSION SWITCHES TO A MORE PRACTICAL FORMAT


REPUBLICAN PARTY
DEBATE
MATSON
eaglecartoons.com CQ ROLL CALL

A Hancock County Democrat

ABOUT

"**A Hancock County Democrat is not approved by any formal organization of the Democratic Party.**

Guest submissions are welcome. Please submit any work you would like to see published here to : Bruce Workman

Correction: In a previous issue I mentioned that Trump is a moron. What I should have said is "Trump is an imbecile." I apologize for any confusion this may have caused