Testimony for Senate Gov. Opss, H.429.,
March 29,2023
Angelo Lynn, editor/publisher of the Addison County Independent, Middlebury, Vt.

Thank you Chair Ruth Hardy and Vice Chair Vyhofsky.

I'm here as an interested citizen concerned about the integrity of Vermont's elections, today, and more importantly in future years as we contemplate ways to expand online voting.

Specifically, I'm here to argue that based on current studies and research conducted by federal agencies dedicated to cyber security, that despite what vendors may tell you, no online voting system is secure. In H.429, the legislation proposes several measures to address minor hiccups in Vermont's election laws and does it well. However, in the brief section of the bill that expands online voting to include the ability to return signed ballots electronically, it invites a risk far greater than the reward.

To that point, I'd urge this committee, and the Legislature, to adopt one overriding goal as you contemplate expanding electronic voting: DO NO HARM.

Make sure that what's approved is absolutely secure, because if it is not 100% guaranteed, you risk undermining the integrity of Vermont's election system, and once trust is lost, it is very difficult to rebuild.

To understand the risk, we must first understand the players.

The state currently contracts with Democracy Live, a technology vendor that already has a contract with Vermont to send out digital ballots to voters with disabilities, and military personnel who are stationed in distant locations. Voters receive those ballots, print them out and return them via mail. It's a system that works well.

The language in the proposed bill, however, would allow voters to return the completed ballot digitally over the Internet. That requires a much more complicated process and a system that is impossible to secure, according to numerous studies, including this 2020 report by four federal agencies: the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology, the Election Assistance Commission and the FBI. They wrote, rather blandly:

"Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results — and can occur at scale."

Or consider this more forceful passage from a recent letter to Vermont legislators (see full letter at bottom of this testimony):

"We (a group of cyber-security experts) noted and share your concerns with internet voting. Internet voting, referring primarily to the electronic return of a marked ballot via email, fax, web-based portal, or mobile apps, is not a secure solution for voting in Vermont or elsewhere in any form, nor will it be in the foreseeable future…

"In April (2022) we wrote to every governor, secretary of state, and state election director across the country detailing the scientific and technical risks of internet voting and urging officials to refrain from allowing the use of any internet voting system. To date, more than 80 leading organizations, scientists, and security experts have signed the letter, which documents that:

- All internet voting systems and technologies are currently inherently insecure.
- No technical evidence exists that any internet voting technology is safe or can be made so in the foreseeable future; rather, all research performed to date demonstrates the opposite.
- No blockchain technology can mitigate the profound dangers inherent in internet voting.
- No mobile voting app is sufficiently secure to permit its use.

It's also important to note that the financial contract with Democracy Live would likely be more expensive with the added service. How much that is should be known to this committee and to all Vermonters, but it's clear that this is a contract is priced to generate a profit for the vendor. To that end, when any vendor sells a complex product it's prudent to acknowledge the Latin saying, Caveat emptor, "let the buyer beware."

Furthermore, as other testimony by online election expert Susan Greenhalgh will explain, trying to secure online voting systems presents unique problems because it's also private, so there's no way a voter or the town receiving that vote will know if it has been tampered with. And once hacked, the votes can be changed and manipulated at scale without any evidence or warning to voting officials, according to the CISA report noted above.

Now, I'm no cyber-security expert, but I can read reports and as an editor I've spent 45 years assessing where there are holes in stories or arguments.

Of the cyber-security reports I've read by several federal agencies, they all reach the same conclusion as noted above. And the federal agencies have tried to create a secure system. It was an 8-year goal of a project directed by Congress and carried out by the National Institute of Standards and Technology. In 2015, they gave up and said it couldn't be done… and that assessment hasn't changed. Just a few months ago, a working group convened by the University of California at Berkeley's Center for Security in Politics concluded after more than a year of research that this hadn't changed, and it could not write standards to secure electronic ballot returns.

One may ask why these reports aren't more front and center, and there's a clear answer: Federal agencies can't advocate for election reforms in state affairs. They can provide studies, but the states themselves must take the initiative to read the studies and make their own decisions.

****

On the other side of this issue, we have a private company that seeks to expand electronic voting services with Vermont and other states across the nation, which will make the company a lot of money — and their proof of security is to say, in a couple of words, "trust us."

When pressed for evidence of their claims, Democracy Live sells the fact that scientific-sounding groups have done studies, but they won't provide any studies done by federal agencies. Nor is this a regulated industry with government oversight.

Certainly, Vermont's Legislature won't accept, "trust us," as an adequate answer. Rather, written peer reviewed studies should be reviewed by committee members, and scrutinized by the federal agencies that specialize in election security or universities like MIT. Why would Vermonters expect anything less?

****

Now, I'm not here to criticize Democracy Live, or its patron Mobile Voting, or its billionaire founder Bradley Tusk, for seeking to provide a secure online voting system with the ultimate goal of improving voter turnout. It IS a noble idea and goal.

If it were possible to make voting easier and more convenient, and get a much higher percentage of Americans casting votes in every election, that would be awesome… And, no doubt that ideal is what's driving this initiative and the legislative effort behind it. We applaud that effort.

And it's been an effective pitch for Democracy Live and other online election vendors. To date, over two-dozen states allow return ballots via the Internet… many of whom made those decisions more than a decade ago before today's security issues were more concerning. Still, the idea of expanding voting opportunity via the internet is compelling and sometimes a quick sell. I hope Vermont will be more cautious.

The 800-pound gorilla on this issue, particularly in today's environment, is the lack of security. And because election results can be manipulated at scale if breached, it doesn't work if it's 95% secure, it has to be as close to 100% as possible because it's that one instance that destroys election credibility.

And make no mistake, there are bad actors out there, including foreign actors, who want nothing more than to weaken our democracy. In contemplating such voting systems, we must consider that expert state actors will, for the foreseeable future, be trying to sow disruption and create a loss of faith in our democracy. California, Utah, Washington, D.C. and others have recently rejected online voting initiatives because of those concerns.

Now, if Democracy Live were to offer a fool-proof guarantee that its system was secure, that would provide more confidence. But they won't. A clause in their typical contract clearly states that they can't be held liable for breaches of security. Section 7.2 states, in all caps: "DEMOCRACY LIVE DOES NOT REPRESENT OR WARRANT THAT SECURE SELECT AND OMNIBALLOT ONLINE WILL

OPERATE ERROR-FREE OR UNINTERRUPTED AND THAT ALL PROGRAM ERRORS IN SECURE SELECT AND OMNIBALLOT ONLINE CAN BE FOUND IN ORDER TO BE CORRECTED. NOR DOES DEMOCRACY LIVE MAKE ANY WARRANTIES REGARDING THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION CONTENT."

https://bosagenda.co.siskiyou.ca.us/335919/335925/365091/365092/365094/2365094.pdf

And I don't blame them. The scientific community says it can't be done, and their contract agrees.

But their sales pitch sings a different tune. Time and again, they emphasize how secure the system is. Legislators must determine if it's a siren's song with ample verbal assurances, but no written proof. Again, caveat emptor.

Knowing, then, that this committee, and ultimately, the Legislature, has to determine the security of the vendor's voting system, here are a few questions Vermonters will want to know:

• How many voters currently receive ballots via email and how many have been returned by mail in previous elections? (Goal: To judge how effective the current system is.)

• How many more voters would be reached under the proposed change? (That is, is the expansion worth the risk?)

• Under the language of this section, it appears that any valid voter seeking an absentee ballot could feasibly receive a blank ballot online and return it online. What's the greatest potential number that might be, and would that overwhelm the ability of town clerks to process those votes in the manner described?

• What's the current monetary value of the contract with Democracy Live, and what would it be with the expanded contract?

• What current voting processes do we have for our military forces, and those with disabilities, and can the problems be solved in other ways with less risk to election integrity?

• Finally, is this matter so pressing that it can't be shelved for a year until these questions are more fully explored?

****

Some of these answers should be easy to ascertain and I'm eager to know those answers. Other questions are more complex, and I certainly appreciate the time and careful consideration this committee is giving the bill.

In conclusion, I would submit that current risks outweigh the benefits, and that the online voting provision in this proposed bill be struck, leaving the current online voting process as is, or modifying the current process by extending the days to receive mailed ballots from military personnel and from voters with disabilities, as was previously suggested by the vice-chair of this committee.

I'm also here to say that as an editor/publisher of the Addison Independent for the past 38 years I sincerely appreciate every legislator's willingness to do this job, always seeking to find solutions to countless problems — and opportunities — facing the state. I understand how time-consuming each issue can be, and how impossible it is to read every article written on both sides of any issue.

I also fully realize that this tiny section of this bill — which simply seeks to make it easier for a few people to vote — doesn't seem like a huge deal in the scale of what's important in this legislative session. But I would argue that it's more important than it may seem. In most ways, it is a very small change, but it also poses a huge risk that could have enormous consequences.

So, again, I ask you to first, DO NO HARM.

Second, to heed the Latin saying, caveat emptor.

And, third, here's a twist on a Reagan quip: "Never trust, always verify." That is especially true when dealing with the integrity of Vermont's elections.

In my written testimony, I've included some additional readings with excerpts and links. Thanks for your time and consideration.

Respectfully,

Angelo Lynn

Additional readings suggested by Angelo Lynn:

1. 1) The Intercept, an online investigative journalism operation, wrote an insightful story on Mobile Voting and its billionaire owner Bradley Tusk. Tusk also owns Democracy Live. To understand who the state is dealing with, it's key to read this story. See the full story here: https://theintercept.com/2022/11/04/election-online-mobile-voting-bradley-tusk/

Here's are some excerpts:

“Time after time, when you ask Democracy Live or its parent, Mobile Voting, for reports to justify any of its claims, none are forthcoming. What owner Tusk is good at is podcasts which he lavishly praises the idea of online, mobile voting, while disparaging anyone who is against it…”

“Ultimately, though, the bill’s lack of specificity may not matter,” says Ron Rivest, a cryptographer at MIT who co-invented one of the most widely used algorithms to securely transmit data. “When people ask for best practices for voting online, it’s rather like asking for best practices for driving drunk,” Rivest says.

Even a grant recipient of Tusk Philanthropies doesn’t believe the practice is safe. “For the foreseeable future iVoting solutions introduce far more risk than benefit because there remain too many technical problems to verifiably solve,” said Gregory Miller, COO and co-founder of the Open Source Election Technology Institute, or OSET, which Miller said received a two-year, $1 million grant from Tusk Philanthropies.

****

In 2020, Tusk donated $40,000 to Shemia Fagan’s campaign to become Oregon’s secretary of state — the most he’s ever donated to a candidate and Fagan’s largest individual donor, according to FollowTheMoney.org. After Fagan won her race and d became the state’s chief election official, a bill was introduced in the state’s legislature to create an internet voting system. The content of the legislation… would’ve put Fagan in charge of creating the rules around the system’s implementation.

Fagan did not support the bill, and the bill did not pass. Fagan told The Intercept her independent judgment was never compromised by Tusk’s donation and that she declined Mobile Voting’s invitation to join its Circle of Advisors, saying she wanted to focus instead on restoring trust in vote by mail. As for her position on internet voting, she says she did meet with representatives from Mobile Voting. “Ultimately, they could not refute the strongest concerns raised by the opponents,” she said.

******

And then there’s this quote that reflects on Tusk’s long-term political strategy for his firm’s development of online voting:

“We’ve either made it available to deployed military or people with disabilities,” Tusk said on a podcast in 2021. “We’ve found one group on the right that no one can object to, and one group on the left that no one can object to.”… Combined, the people casting ballots electronically represented less than .2 percent of all the votes cast in 2020. However, voters with disabilities are increasingly advocating to use those digital options for themselves. And once a right is expanded to one group, another usually follows… Or, as Tusk put it in 2019, “What we learned at Uber is once the genie is out of the bottle, it can’t be put back in.”

****

2. Another source is this letter to VermontUtah legislators from national and state scientists and academics from Vermont Utah opposed to a provision in Utah to expand internet voting. The four bullet points are key:

Re: <u>The Continued Inherent Insecurity of Internet Voting</u>

Dear President Pro Tempore Baruth and Chairwoman Hardy:

We are writing from the American Association for the Advancement of Science's (AAAS) Center for Scientific Evidence in Public Issues and the U.S. Technology Policy Committee of the Association for Computing Machinery (USTPC) regarding the Vermont legislature's consideration of authorizing insecure internet voting. AAAS, the world's largest multidisciplinary scientific society, and ACM, the world's largest computing society, work apolitically to promote the responsible use of science and technology in public policy.

As the Senate considers H. 429, we write to caution unequivocally that ***internet voting*** – referring primarily to the electronic return of a marked ballot via email, fax, web-based portal, or mobile apps – ***is not a secure solution for voting in Vermont or elsewhere in any form, nor will it be in the foreseeable future***. Indeed, those facts have not changed since April of 2020 when we jointly wrote to every governor, secretary of state, and state election director across the country detailing the scientific and technical risks of internet voting and urging officials to refrain from allowing the use of any internet voting system. More than 80 leading organizations, scientists, and security experts also signed that letter, which documents that:

- • All internet voting systems and technologies are inherently insecure.
- • No technical evidence exists that any internet voting technology is safe or can be made so in the foreseeable future; rather, all research performed to date demonstrates the opposite.
- • Blockchain technology cannot mitigate the profound dangers inherent in internet voting.
- • No mobile voting app is sufficiently secure to permit its use.

These statements distill the findings of more than two decades of rigorous, science-based analysis.

In 2020, the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) jointly released additional guidance describing the electronic return of ballots as "high-risk even with controls in place." The guidance explains that "***electronic ballot return, the digital return of a voted ballot by the voter, creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system***… Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time."

These concerns echo a 2018 consensus study report on election security by the National Academies of Science, Engineering, and Medicine (NASEM), the most definitive and comprehensive report on the scientific evidence behind voting security in the U.S. to date, which stated:

> "***At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.*** Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as ***no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet***."

Moreover***,*** despite these profound risks, a recent report by MIT researchers concluded that "online voting may have little to no effect on turnout in practice, and it may even increase disenfranchisement."

We share legislators' desire to expand ballot access for all, but respectfully submit that Vermont can best demonstrate leadership in election security by committing to scientifically sound election systems that embrace both accessibility and security. As noted in these remote voting recommendations, ***more secure alternatives exist to provide accessible remote voting for overseas uniformed personnel and individuals with disabilities, and others who may have difficulty accessing the ballot***.

We would welcome the opportunity to discuss more secure alternatives to internet voting with you and your colleagues, including accessible remote voting by mail, and to connect you with leading experts on these technologies. To arrange for such briefings, please don't hesitate to contact us directly.

Michael D. Fernandez, Director,
Center for Scientific Evidence in Public Issues
American Association for the Advancement of Science
1200 New York Avenue, NW
Wasington, DC 2005
202-326-7056   202-580-6555
mdfernandez@aaas.org

and
Jeremy J. Epstein, Chair
U.S. Technology Policy Committee
Association for Computing Machinery
1701 Penn. Avenue, NW, Suite 200
Washington, DC 20006
202-580-6555
acmpo@acm.org

3. Or this report (https://www.usenix.org/conference/usenixsecurity21/presentation/specter-security) from Michael Specter, MIT; and J. Alex Halderman, University of Michigan, titled: Security Analysis of the Democracy Live Online Voting System.

Here's the introduction to their 16-page report:

"Democracy Live's OmniBallot platform is a web-based system for blank ballot delivery, ballot marking, and online voting. In early 2020, three states—Delaware, West Virginia, and New Jersey—announced that they would allow certain voters to cast votes online using OmniBallot, but, despite the well established risks of Internet voting, the system has never before undergone a public, independent security review.

We reverse engineered the client-side portion of Omni- Ballot, as used in Delaware, in order to detail the system's operation and analyze its security. We find that OmniBallot uses a simplistic approach to Internet voting that is vulnerable to vote manipulation by malware on the voter's device and by insiders or other attackers who can compromise Democracy Live, Amazon, Google, or Cloudflare. In addition, Democracy Live, which had no privacy policy prior to our work, receives sensitive personally identifiable information—including the voter's identity, ballot selections, and browser fingerprint— that could be used to target political ads or disinformation campaigns. Even when OmniBallot is used to mark ballots that will be printed and returned in the mail, the software sends the voter's identity and ballot choices to Democracy Live, an unnecessary risk that jeopardizes the secret ballot.

We recommend changes to make the platform safer for ballot delivery and marking. However, we conclude that using OmniBallot for electronic ballot return represents a severe risk to election security and could allow attackers to alter election results without detection. In response to our findings, Delaware and New Jersey halted their use of OmniBallot for online voting, but it remains available in other jurisdictions, as do similar tools that likely face the same serious risks."