Testimony to the Vermont House Government Operations Committee regarding the term "electronic" voting in the pending elections bill.

3/11/2025

My name is John Odum and I currently serve as City Clerk of Montpelier. In that capacity I am the election administrator for Montpelier and have been so for the past thirteen years. I hold a Certificate of Election Administration from The Humphrey School of Public Affairs at the University of Minnesota and am a Certified Municipal Clerk through the International Institute of Municipal Clerks. Prior to being Clerk, I worked as a political organizer at the state and local level in Vermont and Oregon. Additionally, I have worked in IT administrative capacities for the Vermont Democratic Party and Planned Parenthood of Northern New England. I am a Certified Ethical Hacker (CEH - a penetration tester certification). I am also a Certified Network Defense Architect (CNDA) and a regular presenter at DEF CON, the largest hacker conference in the world, on subjects relating to election security. From that background,

The language under discussion generally restates *current* procedures for overseas voting, and expanding it to disabled voters. The *current* system does not allow for direct voting over the Internet in any way.

My concern is any discussion - even couched in the term "remote" voting - that may emerge relating to "return(ing) ballots electronically" - a phrase that could - and would - include direct "voting online" in some form. As particularly stated in § 2543(d)(1)(a), it could authorize anything from email or filling out a "pdf" to mobile device voting.

On a personal level, I do find the remote (Internet) voting appealing, which is why it breaks my heart to have to present the following concerns and recommend that it not be implemented in any form. My concern is, naturally, ballot security and overall **election integrity**, and to that end, **I recommend the term "electronically" be reconsidered so as not to make direct Internet voting possible.**

It is important for me personally to acknowledge the more immediate problems Internet voting could help alleviate – those are, the challenges of facilitating voting for Americans overseas and the disabled, as well as a measurable increase in turnout. **While the system could help, it's always important that any cure not be more damaging than the disease, and that would be the question before you in a direct Internet voting scenario.** There is a risk/benefit analysis that must be done before deploying such a system at all, let alone on a large scale - and as we can see from the increasing number of pilot projects nationwide, **the "slippery slope" argument is front and center**. Sauce for the goose is always sauce for the gander; should Internet voting be implemented on a small scale, there will be no political argument to prevent it from being expanded universally.

It should be noted that supporters of Internet voting are generally policy experts or activists speaking of how they believe Internet voting has the potential to expand the franchise. On the other side, most of the **vocal opponents of Internet voting are technology experts** from such institutions

as MIT[1] (*"Internet… voting would come at the cost of losing meaningful assurance that votes have been counted as they were cast, and not undetectably altered or discarded"*), Johns Hopkins[2] (*"voting over the Internet…is a non-starter"*), Stanford[3] *("Online Voting Is a Danger to Democracy")*, and even the American Association for the Advancement of Science[4] (" *Over two decades of research have detailed the challenges inherent in creating a secure, secret and verifiable system for voting*"). **I would hate to see Vermont join in with the prevailing national pattern of arbitrary rejections of experts in their fields when critical state and national interests are at stake.**

The simple reality is that the idea suffers from security issues that exist beyond the end-to-end system they deploy. Let me be clear, while I think it's unlikely (certainly not impossible) that votes would be changed (just as a matter of ease and scale of attack vectors), **it is easy to imagine an election being *disrupted in any large-scale implementation*, which can itself change a result if the disruption is large enough**. Disruption is the mantra of the black hat ("bad guy") hacker community.

Many promote Internet voting by comparing it to online banking. The argument goes "if we trust the Internet with our banking, why can't we trust it to vote?" The comparison is telling – though not in the way proponents imply. According to security.org[5], 29% of US adults have experienced some kind of Account Takeover (ATO) attack, and 42% of those were banking accounts - this equates to about 8.400,000. Its security should not be overstated for rhetorical purposes.

But more concerning than the numbers themselves is the simple fact that *everybody knows this*. Everybody knows and takes for granted that a certain amount of successful hacking of Internet banking out there is unavoidable. We are often reminded of this in the media when we receive advice on how to minimize the risk. But as I say, this banking advice is advice to *minimize* the risk, and no one expects it to be *eliminated*.

To accept the same perspective and offer the same shrug or resignation about voting would be an abandonment of one of the most fundamental tenets of elections – that every single vote is precious, and that any lost vote should never be casually accepted. I have concern over what such a change in attitude would mean in the long run.

The worries are those attacks based on vulnerabilities that can impact a lot of voters at once, and this is where Internet voting becomes dangerous.

My real first concern is about **malware** ("trojans" and the like). In 2023, 6.06 billion malware attacks were reported.[6]Over 1 billion malware programs exist, and in terms of mobile devices, would inevitably impact any medium for Internet voting. Some have estimated that 750 million Android mobile devices have been infected, equaling a rate of infection of 4.3%[7] (although I personally

---

[1] https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf
[2] https://www.scientificamerican.com/article/pogue-the-challenges-of-digital-voting/
[3] https://engineering.stanford.edu/news/david-dill-why-online-voting-danger-democracy
[4] https://www.aaas.org/epi-center/Internet-online-voting
[5] https://www.security.org/digital-safety/account-takeover-annual-report/
[6] https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/
[7] https://www.pcmag.com/news/report-android-43-devices-vulnerable-to-bug

believe the number is lower, it is high regardless). If one thinks mobile devices - likely to be a large medium for Internet voting - are immune**, one piece of malware alone infected more than 11 million mobile devices only last year, and a large amount of Internet voting could take place by phone or tablet (such as an ipad)**[8].

The thing about malware is that it can affect the election from *outside* any voting system and therefore be out of its security provisions. There is malware that can uninstall apps (such as potentially the app voters would use to cast their ballot) and replace them with malicious programs, capture personal information, and take control of devices. All of which, actively implemented at a large scale, could disrupt an election and would be out of the reach of any Internet-based election security, even one including biometrics such as facial recognition.

Then there's the biggest, most common, hack of all - phishing. Phishing is incredibly effective. In 2021, a phishing campaign's click rate was 17.8%. Targeted campaigns had an average click rate of 53.2%[9] This kind of attack can make unsophisticated or otherwise unknowing users **go to websites they may think are election related, if they receive malicious email masquerading as official, Secretary of State email. If they understand that Internet voting is a practice, they may click through and believe they are casting a vote and therefore be disenfranchised. There could be identity theft.**

In terms of voting mobile (again, which would be common in a vote-by-Internet scenario), another big concern is "smishing.[10]" Smishing is mobile text "phishing" and can be a way to deliver malware or perform identity theft, which can lead to hacks that transfer a phone number to another device without anyone knowing. Smishing, like windows and ios (apple) phishing, is common and easy, and the rate of people who receive a smishing attack and who click on a malicious link is between 8.9% and 14.5%[11] - and a remote voter can be targeted by micro-targeted smishing campaigns designed to spread false information.

Multifactor identification is robust protection, but as phishing attempts are increasing dramatically, it may not matter.

These are examples of how a malicious user may be able to impact the computer or phone itself and thereby the app large-scale without having to engage with the voting system itself, no matter how secure it may or may not be.

---

[8] https://www.kaspersky.com/blog/necro-infects-android-users/52201/

[9] https://aag-it.com/the-latest-phishing-statistics/#:~:text=In%202021%2C%20the%20average%20click,12%25%20delivered%20malware

[10] https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-smishing/#:~:text=SMS%20phishing%2C%20or%20smishing%2C%20is,%2C%20or%20log%2Din%20password.

[11] https://www.ibm.com/think/topics/smishing#:~:text=Scammers%20choose%20smishing%20over%20other,between%208.9%25%20and%2014.5%25.&text=By%20comparison%2C%20emails%20have%20an,%25%2C%20according%20to%20Constant%20Contact.&text=In%20addition%2C%20scammers%20can%20mask,their%20focus%20to%20smishing%20attacks.

But most concerning for many of us who run polls is the potential use of large-scale Internet voting as a tool for **voter *suppression***. Currently, the use of "robocalls" or automated phone calls, to spread false information which could trick voters into any number of things is common.[12]

Any hackable voter database on the state side, or website portals, could be used to **harvest voter emails or mobile phone numbers to transmit incorrect information about poll locations, or threats of dangers at the polls designed to keep voters away via deceptive texts**. Lists can also be found commercially available. This is the kind of misinformation-spreading that is currently the purview of robocall voter suppression, but the potential scale to which this medium may increase effective misinformation under large-scale mobile elections could potentially be astonishing. Coupled with the fact that enough information exists to micro-target such attacks to historically marginalized communities, the issue can even become a civil rights one in a worst case scenario.

Following up on the above, leaning heavily on such an Internet voting system (and why bother passing it if we're not ultimately planning to?), **we also set ourselves up for potential mischief on the other side of the equation - the servers** where these systems are hosted. These are issues that already exist with states' election management systems and voter databases[13], but **putting more vital tech infrastructure into those same cloud services simply increases the opportunities for potential mischief**. Hosting on Amazon Web Services (AWS) for example, is not a guarantee of success, as cloud malware does exist.

Additionally, while unlikely, **an online voting system server could be targeted by a distributed denial of service (ddos) attack, perhaps on Election Day** when a disproportionate number of users will likely be voting. A focused attack on a cloud server – outside of MVP's end-to-end voting system - could not be completely defended against by that system, no matter how robust it is. Again, this is unlikely but not impossible as the ante keeps being raised by attackers. In 2019, a ddos attack unheard of in scale took down some of Amazon's hosting services[14] for as much as 8 hours - plenty of time to disrupt an election. Amazon services could well be used for hosting such a system.

Finally, and perhaps most significantly, is the question of **voter confidence**. Among many demographics, Internet voting will inevitably be viewed with a lot of skepticism. If enough of any of the above scenarios play out in a public way, confidence in integrity and outcomes could be severely damaged, leading to more damaging social conflicts.

My purpose here is not to stamp out good ideas, but to look beyond the hype. There may be a use for such technology, but the slippery slope is a real thing – and **this bill should not be worded as to allow Internet voting to be only one step away from statewide elections**.

---

[12] https://www.wired.com/story/biden-robocall-deepfake-danger/
[13] https://cyberscoop.com/cyberattack-hits-georgia-county-at-center-of-voting-software-breach/
[14] https://www.securityweek.com/ddos-attack-hits-amazon-web-services/

Thank you for considering my concerns.