WHY INTERNET VOTING IS DANGEROUS

Barbara Simons*

CITE AS: 4 GEO. L. TECH. REV. 543 (2020)

TABLE OF CONTENTS

Internet voting is the return of voted ballots over the Internet, using a computer, a tablet, or a smart phone. The voted ballot may be transmitted via a web portal, as a PDF or other attachment, or as a fax.

I. IF I CAN BANK ONLINE, WHY CAN'T I VOTE ONLINE?

That is a question we have heard repeatedly for many years. What questioners often do not appreciate is that we cannot bank online either—at least not with a guarantee of security. Banks will continue to provide online banking as long as it is less expensive to cover financial losses from

* Retired, IBM Research; Member, Board of Advisors of the U.S. Election Assistance Commission; Board Chair, Verified Voting. Thanks to the *Georgetown Law Technology Review* for their helpful edits. Any mistakes herein are my own.

cyberattacks than to build new buildings and hire new staff. The situation is nicely summarized in a report from the Atlantic Council:

> When a hacker steals money online, the theft is easily discovered. Banks, online retailers, and other companies offering services over the Internet factor in some degree of loss as a cost of doing business online, and generally indemnify their customers against bad actors. Online voting poses a much tougher problem: lost votes are unacceptable. Online voting systems are complex, and any updates often must be separately recertified by election authorities. And unlike paper ballots, electronic votes cannot be "rolled back" or easily recounted. The twin goals of anonymity and verifiability within an online voting system are largely incompatible with current technologies. Russian state-sanctioned hackers, it should be recalled, brought almost all of Estonia's online activities to a halt in 2007 and might do so for online elections as well. Nobody knows whether the DRE [voting] machines or other proprietary voting systems in use elsewhere have already been hacked too.[1]

An electronic vote cannot be "rolled back" because there is no way to know if it is accurate: What the voter sees on her device's screen may differ from what is stored in the device's memory, sent over the Internet, or received at the polling place. Thus, the secret ballot makes it impossible for the voter to verify her ballot.[2]

II. HOW SERIOUS IS THE PROBLEM?

For years, we have been hearing about successful attacks on a variety of institutions, such as Capital One, Google, Facebook, the FBI, Symantec, Marriott, and the Office of Personnel Management (OPM). All of these institutions have significant financial and personnel resources available to

---

[1] PETER HAYNES, ATLANTIC COUNCIL, ONLINE VOTING: REWARDS AND RISKS 2 (2014) https://www.verifiedvoting.org/wp-content/uploads/2014/10/Online_Voting_Rewards_and_Risks.pdf [https://perma.cc/K973-WLXQ].

[2] There is ongoing research that uses encryption to develop "verifiable end-to-end" internet voting systems. *See, e.g.*, U.S. VOTE FOUND., THE FUTURE OF VOTING: END-TO-END VERIFIABLE INTERNET VOTING—SPECIFICATION AND FEASIBILITY STUDY (2015), https://www.usvotefoundation.org/E2E-VIV [https://perma.cc/QML9-EER3]. However, no currently available system, including blockchain voting systems, provide this type of verification. *See* discussion *infra* Part VI.

them to prevent hackers. In contrast, election officials tend to be underfunded and under-resourced with little to no cybersecurity expertise at their disposal. It is highly unlikely that most local election officials would be able to withstand attacks from powerful nation-states, or even from clever local hackers.

Intelligence experts have been warning for several years that our electoral system is under attack:

- "[T]here were multiple, systematic efforts to interfere in our election."
  — Special Counsel Robert Mueller III[3]

- "He [Putin] tried again to muck around in our elections this last month. We are seeing a continued effort around those lines."
  — James Mattis, former Secretary of Defense[4]

- ". . . Russia attempted to interfere with the last election and continues to engage in malign influence operations to this day."
  — Christopher A. Wray, F.B.I. Director[5]

The findings of the intelligence community were reflected in a bipartisan report issued by the Senate Intelligence Committee on October 8, 2019, which stated:

> . . . DHS [Department of Homeland Security] assessed that the [Russian] searches, done alphabetically, probably included all 50 states, and consisted of research on general election-related web pages, voterID information, election system software, and election service companies.[6]

Russia is not the only country capable of conducting cyberattacks on our elections. North Korea famously hacked Sony because of *The Interview*, a

---

[3] *Letting the Report 'Speak for Itself,'* N.Y. TIMES, May 30, 2019, at A16.
[4] Sophie Tatum et al., *Mattis: Putin 'Tried Again To Muck Around In Our Elections'*, CNN (Dec. 1, 2018, 4:20 PM ET), https://www.cnn.com/2018/12/01/politics/mattis-russia-election-interference/index.html [https://perma.cc/D2BH-WKLR].
[5] Connor O'Brien, *FBI Director: Russia 'Continues To Engage In Malign Influence Operations' Against U.S.*, POLITICO (July 18, 2018), https://www.politico.com/story/2018/07/18/fbi-wray-russia-meddling-732337 [https://perma.cc/P7CZ-TKM2].
[6] SELECT COMM. ON INTEL., REPORT ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, S. REP NO. 116-XX, at 8 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [https://perma.cc/HD8P-S8Q6].

comedy about an assassination attempt on Kim Jong-un.[7] A Chinese state-sponsored hacking group is suspected in a cyber campaign targeting U.S. utility companies.[8] On January 3, 2020, Christopher Krebs, Director of the DHS Cybersecurity and Infrastructure Security Agency, warned: "Bottom line: time to brush up on Iranian TTPs [Tactics, Techniques, and Procedures] and pay close attention to your critical systems . . . Make sure you're also watching third party accesses!"[9]

While there is no evidence that votes were changed in 2016, no proper investigation was conducted because (1) there is no national post-election ballot audit or recount, (2) most of our state laws have not been updated to reflect the risks introduced by the use of computers in elections, (3) some state laws actually appear to be designed to inhibit or prevent post-election ballot audits or recounts, and (4) it is currently impossible to recount any type of paperless voting systems, because we do not know if the results stored in the computers' memories accurately reflect the voters' intentions.[10]

III. WHAT ARE SOME OF THE RISKS OF INTERNET VOTING?

As an old cartoon says, "On the Internet, nobody knows you're a dog."[11] As that cartoon suggests, one of the threats of Internet voting, or indeed of any kind of remote voting, is that the ballot could be cast by someone other than the voter.[12] While illegal, this act is unlikely to be prosecuted. Likewise, since the United States does not have a national ID, it is essentially impossible

---

[7] Richard Stengel, *The Untold Story of the Sony Hack: How North Korea's Battle With Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016*, VANITY FAIR (Oct. 6, 2019), https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack [https://perma.cc/X4HE-DP2L].

[8] Zac Doffman, *Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities*, FORBES (Aug. 3, 2019, 2:31 AM EDT), https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#6f942b5d6758 [https://perma.cc/HV3F-4NFU].

[9] Sergiu Gatlan *U.S. Government Issues Warning About Possible Iranian Cyberattacks*, BLEEPING COMPUTER (Jan 3, 2020), https://www.bleepingcomputer.com/news/security/us-government-issues-warning-about-possible-iranian-cyberattacks/ [https://perma.cc/62B8-H465].

[10] In addition to voter marked paper ballots and laws that require post-election ballot audits and/or recounts, voters must check their paper ballots—especially if the ballots have been produced by machines—and there must be a secure chain of custody of those ballots. These are all important issues, but they are not the focal points of this paper.

[11] The cartoon, by Peter Steiner, was published in *The New Yorker* on July 5, 1993. *See also* Glenn Fleishman, *Cartoon Captures Spirit of the Internet*, N.Y. TIMES, Dec. 14, 2000, at G8.

[12] Internet voting is the return of voted ballots over the Internet, using a computer, a tablet, or a smart phone. The voted ballot may be transmitted via a web portal, as a PDF or other attachment, or as a fax.

to authenticate a potential voter.[13] Other threats include: voter coercion and vote buying/selling, malware on the voter's device that can change or discard the voter's selections without the voter's knowledge, "man-in-the-middle" attacks that intercept the voter's ballot as it is traversing the Internet, and denial of service attacks that can prevent ballots from reaching election officials.

Despite the threats and multiple warnings, there are no regulations governing Internet voting, primarily because no one knows how to write them. In particular, there are no standards (federal or state) regarding independent testing, government oversight, legal accountability, or indeed the ability to conduct a recount.

The National Institute of Standards and Technology (NIST) was asked to develop Internet voting standards, but has not done so.[14] Instead, NIST produced reports that warned about threats to Internet voting. One such report states:

> In addition, the platforms not under the control of election officials [i.e. the voter's computer or smart phone] may be poorly protected and vulnerable to malware, phishing, and denial of service attacks. These platforms may be the target of attacks to monitor and/or modify voter choices, capture personal information, or prevent a voter from accessing the voting services . . . . When voting platforms contain malware, the voting platform may try to inhibit a voter from casting his or her ballot, alter a voter's choices, monitor how a voter votes, use the voter's credential to gain and expand access to damage the voting system, change election results, or harm the credibility of the election results.[15]

NIST has consistently warned of the dangers of Internet voting, as a recent website posting exemplifies: "Malware on voters' personal computers

---

[13] There are claims that smart phones can be used to authenticate voters. We discuss those claims later in the paper. *See* discussion *infra* Part VI.

[14] NIST is authorized "to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure." Dr. Charles H. Romine, Dir. Information Technology Laboratory, NIST, *Election Security: Voting Technology Vulnerabilities* (June 25, 2019) (testimony before H. Subcomm. on Research and Tech.), https://www.nist.gov/speech-testimony/election-security-voting-technology-vulnerabilities [https://perma.cc/N2KB-A8UE].

[15] NELSON HASTINGS ET AL., NIST SECURITY CONSIDERATIONS FOR REMOTE ELECTRONIC UOCAVA VOTING 9–10 (2011), https://www.nist.gov/system/files/documents/itl/vote/NISTIR-7700-feb2011.pdf [https://perma.cc/8F9R-DEME].

poses a serious threat that could compromise the secrecy or integrity of voters' ballots."[16]

IV. HOW SECURE ARE INTERNET VOTING SYSTEMS?

A. The District of Columbia

The first example of an Internet voting system that was subjected to independent testing was the 2010 "digital vote by mail" pilot project in Washington, DC. The system, which was developed by the Open Source Digital Voting Foundation, aimed to provide Internet voting for UOCAVA voters.

The District of Columbia Board of Elections and Ethics (BOEE) took the enlightened and unusual path of providing a "public review period" during which anyone was allowed to attempt to break into a mock election.[17] The public testing was scheduled to run from late September to early October. However, by October 1, voters in the mock election were hearing the University of Michigan Fight Song played after they cast their ballots. The song turned out to be the "calling card" of the university team that had successfully broken into the system within 36 hours of the start of the test. Of course, an intruder wishing to manipulate an election would not be so obvious.

The Michigan team, under the leadership of Professor Alex Halderman, was able to modify previously cast ballots, rig subsequently cast ballots, and reveal voters' selections, thereby violating the voters' right to a secret ballot. They even controlled the network infrastructure for the pilot and were able to watch network operators configure and test the equipment. When the Michigan team observed attempted break-ins that appeared to be from China and Iran, they protected the system from those break-ins.[18]

B. The City of Toronto

In 2014 Toronto issued a Request for Proposal (RFP) for Internet voting which mandated that vendors competing for the contract first submit

---

[16] *NIST Activities on UOCAVA Voting*, NIST (Nov. 15, 2019), https://www.nist.gov/itl/voting/nist-activities-uocava-voting [https://perma.cc/3VJ2-SB43].

[17] Attempting to break into a real election, even if the intent is to expose vulnerabilities, is illegal. The information about this exercise is taken from Scott Wolchok et al., *Attacking the Washington, D.C. Internet Voting System*, *in* PROC. 16TH CONFERENCE ON FINANCIAL CRYPTOGRAPHY & DATA SECURITY 114 (2012). See also J. Alex Halderman, *Hacking the D.C. Internet Voting Pilot*, FREEDOM TO TINKER (Oct. 5, 2010), https://freedom-to-tinker.com/2010/10/05/hacking-dc-internet-voting-pilot/ [https://perma.cc/HA2U-ECN5] for a less technical explanation.

[18] Wolchok et al., *supra* note 17, at 10.

their systems for security examination by independent experts. Since vendors typically do not provide their systems for independent inspection, the Toronto RFP—which should be typical—was quite unusual.

The independent experts recommended against the purchase of any of the submitted systems:

> Of the proposals evaluated in the context of the RFP process, it is our opinion that no proposal provides adequate protection against the risks inherent in internet voting. It is our recommendation, therefore, that the City *not* proceed with internet voting in the upcoming municipal election.[19]

The Toronto study is one of the few examples of an independent assessment of commercial Internet voting systems.

C. Estonia

In March 2007 Estonia became the first country to authorize Internet voting in a national parliamentary election. (Voters still had the option of casting paper ballots.) In April 2007, Estonia suffered massive cyberattacks that in some cases lasted weeks and appeared to have originated in Russia.[20] While Estonia is often used as an example of how Internet voting can work, this depiction fails on several counts, as discussed below.

Estonian cryptographer Helger Lipmaa explained why he was casting a paper ballot:

> Voter computers are an obvious problem: most of the people are computer illiterate, and are not able to check if their computers are not infected. Even if they have the newest antivirus (which we can't be sure of), that antivirus itself might not be able to detect a piece of new malware that has been written specifically for *that* election and is unleashed just before it.[21]

---

[19] JEREMY CLARK & ALEKSANDER ESSEX, INTERNET VOTING FOR PERSONS WITH DISABILITIES–SECURITY ASSESSMENT OF VENDOR PROPOSALS: FINAL REPORT 178 (2014), https://www.verifiedvoting.org/wp-content/uploads/2014/09/Canada-2014-01543-security-report.pdf [https://perma.cc/CK4S-BMT6].

[20] Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), https://www.bbc.com/news/39655415 [https://perma.cc/W6TZ-MEAP].

[21] Helger Lipmaa, *Paper-Voted (And Why I Did So)*, WHO GROKS IN BEAUTY? (Mar. 5, 2011), https://helger.wordpress.com/2011/03/05/ [https://perma.cc/YP3R-89PL].

In 2011, the mayor of Tallinn, who also was the country's first prime minister, invited me to visit Estonia. As the leader of Estonia's second largest political party, the Centre Party, he and his colleague were concerned that Internet voting was being used to undermine election results in favor of the Reform Party. While I could not determine whether or not election rigging had occurred, during my visit, I expressed a number of concerns relating to the vulnerability of voters' computers to election rigging malware, insider threats, the possibility that the system could have been attacked by anyone anywhere, the lack of transparency (the software was not publicly available), and the lack of a security evaluation by independent computer security experts.[22]

More precise threats were uncovered in 2014 when a group of independent security experts studied the system and concluded that:

> . . . there are multiple ways that state-level attackers, sophisticated online criminals, or dishonest insiders could successfully attack the Estonian I-voting system. Such an attacker could plausibly change votes, disrupt elections, or cast doubt on the integrity of results. These problems are difficult to mitigate, because they stem from basic architectural choices and fundamental limitations on the security and transparency that can be provided by procedural controls. For these reasons, we recommend that Estonia discontinue the I-voting system.[23]

Perhaps most disturbing is the distrust by a major Estonian political party of election results engendered by Internet voting. Because it is impossible to validate the results of an Internet election, it also is impossible to determine whether or not election rigging has occurred. This is a very unhealthy situation for any democracy, especially a relatively new one.

V. WHAT ARE THE ARGUMENTS FOR INTERNET VOTING?

Proponents of Internet voting argue that it is needed for overseas military voters, voters with disabilities, and to increase voter participation.

---

[22] Barbara Simons, *Verified Voting Blog: Report on the Estonian Internet Voting System*, VERIFIED VOTING (Sept. 3, 2011), https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/ [https://perma.cc/Q5UM-3MGV].

[23] J. ALEX HALDERMAN ET AL., SECURITY ANALYSIS OF THE ESTONIAN INTERNET VOTING SYSTEM 1 (2014), https://www.verifiedvoting.org/wp-content/uploads/2014/10/Estonia_2014_IVotingReport.pdf [https://perma.cc/ML6T-KRXA].

A. Military Voters

In 1986 Congress passed the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA).[24] Consequently, military and overseas voters often are referred to as UOCAVA voters.

The 2009 Military and Overseas Voter Empowerment Act (MOVE) significantly sped up ballot delivery to UOCAVA voters.[25] MOVE requires states to make blank ballots available electronically at least 45 days before an election. The voter can download the ballot, print it out, mark it, and return the voted ballot by postal mail. MOVE also provides free expedited mail service for voted ballots of overseas uniformed service voters. While there are security risks with the online posting of blank ballots, those risks are dwarfed by the risks of returning voted ballots over the Internet.

MOVE has made it possible for almost all military voters to return their voted ballots in a timely fashion, as was confirmed by an analysis conducted shortly after the passage of MOVE by the Military Postal Service Agency (MPSA):

> Election officials must adhere to the MOVE Act requirement for dispatching absentee ballots to voters no later than 45 days prior to the election date. This provides adequate time for ballots to reach absentee voters in the most remote locations to vote and mail back their ballot for the election.[26]

Inevitably, there will be a small number of service people who will be unable to return their voted ballots in a timely fashion. These cases are sometimes used to demand Internet voting for UOCAVA voters—instead of calling for extending the date for receipt of voted ballots, as has been done by several states. As a result, and despite multiple warnings, Internet voting is allowed in approximately 30 states, primarily for UOCAVA voters.

---

[24] *The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)*, U.S. DEPT. JUSTICE (Feb. 26, 2020), https://www.justice.gov/servicemembers/uniformed-and-overseas-citizens-absentee-voting-act-uocava [https://perma.cc/5SNE-PASG].

[25] Press Release, No. 10-1212, Dep't of Justice, Fact Sheet: Move Act (Oct. 27, 2010), https://www.justice.gov/opa/pr/fact-sheet-move-act [https://perma.cc/AT4D-8694].

[26] MILITARY POSTAL SERV. AGENCY, THE 2010 ANALYSIS OF THE MILITARY POSTAL SYSTEM COMPLIANCE WITH THE MOVE ACT, at 8-1 (2010), https://web.archive.org/web/20120915111550/http://www.fvap.gov/resources/media/2010_MPSA_after_action_report.pdf [https://perma.cc/DG6W-GJ2S].

B. Voters with Disabilities

The 2002 Help America Vote Act (HAVA), which allocated almost $4 billion for the purchase of new voting systems, also required that polling places provide an accessible voting system for voters with disabilities.[27] In part because of the explicit mention of Direct Recording Electronic (DRE) machines in HAVA, the bulk of the early post-HAVA systems were DREs that stored the voted ballot in the memory of the machine. Many of these systems were paperless, providing no opportunity to check the accuracy of the results.[28]

Vendors claimed that the DREs were secure, though we have known since the first independent security study of DREs that they have significant vulnerabilities.[29] Vendors also claimed that the DREs were easy for voters with disabilities to use, thereby satisfying the HAVA requirement for accessible voting systems.[30] The accessibility claim, however, turned out to have been an exaggeration at best. For example, the California Secretary of State's 2007 Top-to-Bottom Review of California voting machines examined the accessibility of those machines:

> Although each of the tested voting systems included some accessibility accommodations, none met the accessibility requirements of current law and none performed satisfactorily in test voting by persons with a range of disabilities and alternate language needs.[31]

---

[27] Help America Vote Act of 2002, 52 U.S.C. § 21081 (a)(3)(A) (2020).

[28] When there was an outcry against the paperless DREs, vendors developed a retrofit called Voter Verified Paper Ballots (VVPATs). For a host of reasons, including that voters tended not to check the VVPATs, these machines turned out to be, at best, marginally better than the paperless DREs. We still are coping with the HAVA legacy today. Only Louisiana remains entirely paperless as of this writing, but many other states have paperless jurisdictions, making it impossible to conduct post-election ballot audits or recounts in those states. *See The Verifier—Polling Place Equipment—November 2020*, VERIFIED VOTING, https://www.verifiedvoting.org/verifier/ [https://perma.cc/K5SN-BS8M].

[29] *See, e.g.*, Tadayoshi Kohno et al., *Analysis of an Electronic Voting System*, *in* IEEE SYMPOSIUM ON SECURITY AND PRIVACY 2004 (IEEE Comput. Soc'y Press 2004), https://avirubin.com/vote.pdf [https://perma.cc/96NJ-NE4P].

[30] 52 U.S.C. § 21081 (a)(3)(A) ("The voting system shall be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters . . . ").

[31] NOEL RUNYAN & JIM TOBIAS, ACCESSIBILITY REVIEW REPORT FOR CALIFORNIA TOP-TO-BOTTOM VOTING SYSTEMS REVIEW 1 (2007),

Vendors producing new Ballot Marking Devices (BMDs) also state that the BMDs have good accessibility features. While there has not been much accessibility testing of commercially available BMDs, a Pennsylvania Department of State examination of the ExpressVote XL manufactured by ES&S, the largest national voting system vendor, found three classes of accessibility problems and concluded that "[v]erification is possible, but challenging."[32] These included display problems that do not make the text sufficiently large for low vision users, a lack of information for blind voters such as announcing the party of each candidate, and an inability of blind voters or those with severe vision impairment to verify their ballots. For example, because the XL "displays the printed ballot under a glass panel, and then casts the ballot by automatically depositing the paper ballot in a container while it records the vote electronically," it is "impossible for voters to use personal technology such as magnifiers or text readers to read the paper ballot."[33]

Not surprisingly, a number of disability rights advocates, as well as Internet voting proponents, argue that Internet voting will facilitate voting by those with disabilities.[34] They observe that voters with disabilities can be confronted with numerous obstacles if they attempt to cast their ballots at the polls. These include polling places that are difficult (or even impossible for wheelchairs) to navigate, a lack of facilities for voters with mobility limitations, and voting systems that fail to provide adequate disability accommodations.[35]

Fortunately, we do not need to repeat the mistakes of the past by providing insecure or inadequate voting systems for voters with disabilities, namely Internet voting. Technology exists that allows voters with disabilities to download a blank ballot, mark it from home using their accessibility technology, print the voted ballot, and then return it via postal mail.[36] While

---

https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review/accessibility-review-report-california-top-bottom-voting-systems-review/#LinkTarget_4226 [https://perma.cc/3ZKK-T2QE].

[32] COMMONWEALTH OF PA. DEP'T OF STATE, REPORT CONCERNING THE EXAMINATION OF RESULTS OF ELECTIONS SYSTEMS AND SOFTWARE EVS 6021 WITH DS200 PRECINCT SCANNER, DS450 AND DS850 CENTRAL SCANNERS, EXPRESSVOTE HW 2.1 MARKER AND TABULATOR, EXPRESSVOTE XL TABULATOR AND ELECTIONWARE EMS 18 (2018), https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/ESS%20EVS%206021/EVS%206021%20Secretary%27s%20Report%20Signed%20-%20Including%20Attachments.pdf [https://perma.cc/NZ7A-AJLH].

[33] *Id.* at 19.

[34] *See* DOUGLAS W. JONES & BARBARA SIMONS, CTR. FOR THE STUDY OF LANG. & INFO., STAN. U., *Chapter 9 (Voters with Disabilities)*, *in* BROKEN BALLOTS: WILL YOUR VOTE COUNT? (2012).

[35] See blind voter Noel Runyan's description of voting on an early DRE in *id.* at 216–17.

[36] For voters with disabilities who choose to vote in person at a polling place, there is at least

not perfect, this is far more secure than Internet voting and is deployed in several states, including Oregon and California.[37]

C. Increased Voter Participation

The argument for Internet voting that appears to have the most general appeal is that it will increase voter participation. However, not only is there no evidence that Internet voting increases voter participation, there is substantial evidence to the contrary.

The parliament of British Columbia, Canada, allocated roughly $420,000 (Canadian dollars) for a study on Internet voting.[38] The report recommended against Internet voting at the time it was written and warned that "There are significant risks to implementing Internet voting that can jeopardize the integrity of an election . . ."[39] Among other findings, it dispelled the myth that Internet voting increases voter participation:

> While there have been some Internet voting elections where voter turnout has increased, when other factors such as the apparent closeness of the race and interest in particular contests (e.g., a mayoral election without an incumbent) are taken into consideration, research suggests that Internet voting does not generally cause non-voters to vote. Instead, Internet voting is mostly used as a tool of convenience for individuals who have already decided to vote.[40]

Much to many people's surprise, the report did not find that Internet voting increased participation by young people:

> Researchers have also looked at the demographics of Canadian voters who have used Internet voting and have found that Internet voting is most popular among middle-age voters *and*

---

one BMD that prints a full size paper ballot with the voter's selections that is designed to look like a hand marked paper ballot, thereby making it difficult to distinguish ballots marked by voters with disabilities from other ballots and protecting the secret ballot. *See* Marketing Brochure, Verity Touch Writer: Ballot Marking Device by Hart InterCivic (2016), https://www.hartintercivic.com/wp-content/uploads/VerityTouchWriter.pdf [https://perma.cc/FQ7E-7BUD].

[37] *See Our Story,* FIVE CEDARS GROUP, http://www.fivecedarsgroup.com/#ourstory [https://perma.cc/EL4N-YYLK].

[38] INDEP. PANEL ON INTERNET VOTING B.C., RECOMMENDATIONS REPORT TO THE LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA 7 (2014), https://elections.bc.ca/docs/recommendations-report.pdf [https://perma.cc/2VLV-VGWU].

[39] *See id.* at 47.

[40] *Id.* at 12.

> *least popular among youth and therefore reflects traditional voter turnout demographics*. These findings run contrary to the widely expressed belief that Internet voting will lead to increased participation by youth.[41]

Another notable example is that of Estonia, which has allowed Internet voting since 2005. Recent figures show that voter turnout has declined from 60.6% in 2009 to 53.3% in 2017; turnout in the last Parliamentary election also declined from 64.2% in 2015 to 63.7% in 2019.[42]

In another example, no significant impact on turnout was detected when Switzerland allowed Internet voting in the cantons of Geneva and Zurich in its federal elections from 2004 to 2014.[43]

In sum, Internet voting appears to be a solution in search of a problem—it is not needed for military voters, there are better and safer options for voters with disabilities, and it does not appreciably increase voter participation.

VI. DOES BLOCKCHAIN MAKE INTERNET VOTING SAFER?

A blockchain is a distributed data structure that could have single or multiple owners. In the case of multiple owners, a majority must agree before a transaction is added to the blockchain. Both ownership arrangements have their own vulnerabilities. For example, colluding owners could determine which transactions are added, including possibly false ones. Furthermore, outside attackers who penetrate the servers containing the blockchain might be able to manipulate transactions. But because, blockchain voting is likely to have a single owner—namely the local election official or the vendor—any advantage of having multiple owners that keep a check on each other is eliminated.[44]

---

[41] *Id.* at 13 (emphasis added).

[42] Richard Akerman, *Internet Voting Doesn't Increase Turnout in Estonian Elections*, PAPER VOTE CANADA 2 (Mar. 5, 2019), https://papervotecanada2.wordpress.com/2019/03/05/internet-voting-doesnt-increase-turnout-in-estonian-elections/ [https://perma.cc/JC2A-V3YX].

[43] Katherine Stewart & Jirka Taylor, *Online Voting: The Solution to Declining Political Engagement?*, RAND BLOG (Mar. 23, 2018), https://www.rand.org/blog/2018/03/online-voting-the-solution-to-declining-political-engagement.html [https://perma.cc/2ZVD-7QEC]; *see also* Micha Germann & Uwe Serdült, *Internet Voting and Turnout: Evidence from Switzerland*, 47 ELECTORAL STUD. 1 (2017).

[44] *See* DAVID JEFFERSON, THE MYTH OF "SECURE" BLOCKCHAIN VOTING (2018), https://www.verifiedvoting.org/wp-content/uploads/2018/10/The-Myth-of-_Secure_-Blockchain-Voting-1002.pdf [https://perma.cc/Q4GZ-9D36]; DAVID JEFFERSON ET AL., WHAT WE DON'T KNOW ABOUT THE VOATZ "BLOCKCHAIN" INTERNET VOTING SYSTEM

But one of the largest issues with blockchain voting is that, at its core, blockchain voting is still Internet voting.[45] The National Academy of Sciences produced a report on voting security that warned about these issues:

> Conducting secure and credible Internet elections will require substantial scientific advances. The use of blockchains in an election scenario would do little to address the major security requirements of voting, such as voter verifiability. The security contributions offered by blockchains are better obtained by other means. In the particular case of Internet voting, blockchain methods do not redress the security issues associated with Internet voting.[46]

As suggested by the National Academy, since a voted ballot is transmitted over the Internet, blockchain voting is Internet voting, regardless of what vendors claim. Nonetheless, one of the largest blockchain voting vendor, Voatz, refers to blockchain Internet voting as "mobile" (as opposed to "traditional") voting and downplays the Internet voting aspect:

> While there are different definitions that may come to mind for "Internet Voting", the term typically refers to a browser residing primarily on a voter's PC connected over the Internet to a web server. There are several key differences between traditional Internet voting and Voatz. First, only recently-manufactured smartphone models from Apple, Samsung and Google are supported with Voatz. These devices are built with security features, like fingerprint and facial recognition, that extend far beyond standard browsers running on a potentially-compromised PC for voter authentication. Second, modern smartphones provide hardware-based security to store private keys which, in turn, allow highly secure, encrypted transactions to be conducted over the public Internet. Third, votes are stored on a permissioned blockchain that will eventually be controlled by various stakeholders (e.g. a Secretary of State or a state

(May 1, 2019), https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf [https://perma.cc/TF29-AD4X].

[45] *See* JEFFERSON, THE MYTH OF "SECURE" BLOCKCHAIN VOTING, *supra* note 44.

[46] NAT'L ACAD, OF SCI'S, ENG'G, AND MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 105 (2018).

> board of elections) to ensure their tamper resistance and immutability. [47]

The fact that voters are casting their ballots using smartphones does not address the multiple security threats of Internet voting. While the smartphones mentioned by Voatz use biometrics to authenticate the users, neither the authentication nor the encryption protect against potential vote rigging malware on the phone, as appears to have happened with Jeff Bezos. Bezos claims that malware was introduced into his Apple iPhone X by Mohammed bin Salman.[48]

Furthermore, the fact that a cell phone recognizes its user's biometrics does nothing to ensure that the voter is who she claims to be while authentication questions in general raise privacy concerns. Because we do not have the infrastructure to securely authenticate a remote voter, and because personally identifiable information is needed in order to validate a voter, it is likely that authentication and privacy will be linked in ways that put the voter's private information at risk, especially with smart phone voting. Passwords are not reliable, since most users' passwords are insecure and relatively easy to break. Much personal information, such as SSN, driver's license number, birthdate, etc. has been stolen in massive data breaches and can be purchased, making this information untrustworthy as a tool to validate voters online. The biometrics used by a smart phone to validate the phone owner is not an option, because the biometric information is stored in the phone's memory to which election officials do not have access—nor should they for privacy reasons.

VII. WHAT ARE THE THREATS TO BLOCKCHAIN VOTING SYSTEMS?

Voatz had dominated the market of blockchain voting on smart phones, though that may change because of some recent negative security reports.[49] I discuss how Voatz purports to work, those security reports and additional warning signs, and where the industry is moving now, below.

---

[47] *Frequently Asked Questions,* VOATZ, https://voatz.com/faq.html [https://perma.cc/SLV6-EN25].

[48] Sheera Frenkel, *How Jeff Bezos' iPhone X Was Hacked*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/jeff-bezos-hack-iphone.html [https://perma.cc/9HYS-MZJ6].

[49] *See* MICHAEL A. SPECTER, JAMES KOPPEL, & DANIEL WEITZNER, THE BALLOT IS BUSTED BEFORE THE BLOCKCHAIN: A SECURITY ANALYSIS OF VOATZ, THE FIRST INTERNET VOTING APPLICATION USED IN U.S. FEDERAL ELECTIONS 5 (Internet Pol'y Res. Initiative, Mass. Inst. Tech., 2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf [https://perma.cc/AYM5-6NYA]; *Our Full Report on the Voatz Mobile Voting Platform*, TRAIL OF BITS BLOG (Mar.

A. Voatz

A voter using Voatz casts her vote on her smart phone.[50] Her voted ballot is sent over the Internet to one or more of the thirty-two Voatz blockchains, half of which are on the Microsoft Azure service and half on Amazon Web Services. There is no publicly available information as to how well those blockchains are protected against attack.

Voatz has not stated publicly what the contents of the blockchains are. For example, in addition to the actual ballots, Voatz has not stated what information about the voters, if any, it stores together with the ballots. Voatz claims to use cryptography, but they do not name the encryption scheme used nor where it is used in the process.

Once the election is over, the ballots in the blockchain are decrypted and sent to the local jurisdictions, where they are then printed out and included with the other ballots. Voatz provides no explanation of how this process works.

Voatz asserts that the voter can verify her ballot, but again it does not explain how that is done, nor even what is meant by "verify." It appears that the voter is supposed to be able to determine what votes were recorded for her in the blockchain, but this is not at all clear. Nor is there any description of how the verification is conducted. Is the voter's identity or some other form of ID address stored with her ballot? If so, how is the secrecy of her ballot protected? If she attempts to verify her ballot, how is that information transmitted to her?

Voatz claims to produce a paper trail:

> [A] paper ballot is generated on election night for every mobile vote recorded on the blockchain and the printed ballots are tallied using the standard counting process at each participating county. This also facilitates a post-election audit by comparing the paper ballots with the anonymized voter-verified digital receipts generated at the time of vote submission. [51]

The paper trail/audit claim is grossly misleading since, as we have observed, there is no way to know that the paper printout of the mobile vote accurately reflects the voter's selections.

13, 2020), https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/ [https://perma.cc/RV5W-WW2R].

[50] Much of what follows was found by parsing the *Frequently Asked Questions* page on Voatz.com and through my own observations. *Frequently Asked Questions*, *supra* note 47.

[51] *Id.*

Voatz has never been certified, not least of all because there are no certification standards for Internet voting. However, Voatz does collect and transmit voted ballots, and therefore is a critical voting system component.

Voatz may have a significant negative impact on voters' privacy. Voatz claims to have a method of authentication that involves sending a live facial video together with a photo of the voter's passport photo page or driver's license (front and back) to Jumio, a Palo Alto, California company.[52] Jumio also collects a vast amount of personal information from the voter including name, address, birthday, driver's license or passport number, smart phone number, a copy of the voter's signature, etc.[53] The data collection raises a host of questions, including: Who has access to the data? How secure is it? How long is it retained? What rights does the voter have to determine how the data is used? Is it shared with any other entity? What legal responsibilities do Voatz and Jumio have if the data is inappropriately used, sold, or stolen?

Jumio deploys machine learning to authenticate the voter, but we don't have data about the accuracy of the authentication.[54] Does it have different success rates on different groups, such as people of color? What recourse is there if the voter is wrongly rejected (false negative)? How likely is the software to wrongly authenticating a voter (false positive)? Is the data encrypted? If so, what type of encryption is used? Apparently, there can be human intervention in the case of a failure to match, but details of what that entails are not provided.

Perhaps most disturbing is the Jumio User Information License. Here is part of that license:

> Customer hereby grants to Jumio a license to use, reproduce, modify, create derivative works from, distribute, perform, transmit, anonymize and display the User Information (*including any rights specifically pertaining to biometric information*) necessary to develop, provide and improve the Services, including the right for Jumio to grant equivalent rights to its service providers that perform services that form part of or are otherwise used to perform the Services.[55]

---

[52] SPECTER, KOPPEL, & WEITZNER, *supra* note 49, at 5.

[53] *Id.* at 6.

[54] *See* Jumio Corporation, *About*, JUMIO.COM, https://www.jumio.com/about/ [https://perma.cc/8GU9-XJRF].

[55] Jumio Corporation, *Jumio Terms and Conditions v5.1*, JUMIO.COM § 3.3 (Mar. 17, 2020), https://www.jumio.com/legal-information/terms-and-conditions/v5-1/ [https://perma.cc/A9JZ-XWMF] (emphasis added).

Even though each voter is probably unaware of Jumio's role in the process, Jumio's license purports to give the company control over that voter's data.[56] Though Jumio claims compliance, it is unclear if these license conditions comply with California's new privacy law in practice.[57]

The Jumio license also forbids its customer—Voatz—from reverse engineering of the system for any reason, which would include (unauthorized) independent security testing. Further, Jumio's license also obligates Voatz to prevent other persons—which including voters—from accessing Jumio's product, even if accessing is part of an individual's effort to delete that individual's personal information.[58]

Despite the lack of transparency, Voatz has conducted "pilots" (with real ballots in real governmental elections) in West Virginia during the 2018 primary and midterm and the City and County of Denver municipal general election in 2019. In both cases participation in the pilots was available to UOCAVA voters only. We do not know whether any of the pilot elections was audited—and if so, what the results were.

B. Security Issues

In early 2020 the MIT News Office announced that some MIT researchers had discovered vulnerabilities in Voatz software that would allow "hackers to alter, stop, or expose how an individual user has voted."[59] Voatz responded by calling the researchers' report "flawed."[60] Based on the MIT study, West Virginia terminated their relationship with Voatz and instead announced that they would be using Democracy Live for their online voting.[61]

Voatz also took the unusual step of hiring an outside security firm, Trail of Bits, to assess their product. Still more uncommon, Voatz released the report when it was finalized, even though it was very negative:

---

[56] *See* SPECTER, KOPPEL, & WEITZNER, *supra* note 49, at 7.

[57] *See CCPA Compliance*, JUMIO.COM, https://www.jumio.com/compliance-regulations/ccpa-compliance/ [https://perma.cc/BSJ3-S6VJ].

[58] *See Jumio Terms and Conditions v5.1*, *supra* note 55, at §§ 3.4, 3.6.

[59] SPECTER, KOPPEL, & WEITZNER, *supra* note 49; *see also* Abby Abazorius, *MIT Researchers Identify Security Vulnerabilities in Voting App,* MIT NEWS OFF. (Feb. 13, 2020), http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213 [https://perma.cc/AHM2-NMQN].

[60] *Voatz Response to Researchers' Flawed Report*, BLOG @ VOATZ (Feb. 13, 2020), https://blog.voatz.com/?p=1209 [https://perma.cc/FZ2J-8BHR].

[61] Anthony Izaguirre, *After Damaging Report, W.Va. Moves Away From Voting App*, ASSOCIATED PRESS (Mar. 2, 2020), https://apnews.com/5cafe205322a0abcb3f359f1ea40847f [https://perma.cc/4UJ8-CL6L].

> Our security review resulted in seventy-nine (79) findings. A third of the findings are high severity, another third medium severity, and the remainder a combination of low, undetermined, and informational severity.[62]

Voatz, which is funded by venture capital firms including one associated with Overstock.com, has received substantial financial help from Tusk Holdings and Tusk Philanthropies, founded by its entrepreneur Bradley Tusk.[63] The President of Tusk Philanthropies is Sheila Nix, former Chief of Staff to Dr. Jill Biden. Nix continues to push for expanding blockchain and mobile voting.[64] Tusk Philanthropies was instrumental in helping to arrange Voatz's pilot in West Virginia both by advocating for the company and by providing $150,000 for the test.[65] But West Virginia is not the only "pilot"; Tusk Philanthropies has stated that as of May 2020 they have "successfully completed fourteen pilots in five different states."[66]

It appears that Tusk Philanthropies may have turned away from Voatz, because of the bad security assessments, and instead is supporting another Internet voting system called OmniBallot, produced by Democracy Live.[67] In February, 2020 Tusk Philanthropies partnered with the King County (Seattle) Elections to support an online voting election using Omniballot in a local board supervisor election.[68]

However, Omniballot has some of the same issues as Voatz. An Omniballot FAQ makes the false claim that "OmniBallot is not an online voting system" because "a paper ballot is downloaded by the elections

---

[62] *Our Full Report on the Voatz Mobile Voting Platform*, TRAIL OF BITS BLOG (Mar. 13, 2020), https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/ [https://perma.cc/RV5W-WW2R].

[63] *See* Sue Halpern, *The Campaign for Mobile Voting Is Getting a Midterm Test*, NEW YORKER (Oct. 22, 2018), https://www.newyorker.com/tech/annals-of-technology/the-campaign-for-mobile-phone-voting-is-getting-a-midterm-test [https://perma.cc/N4MB-ZMW5].

[64] Mike Murphy, *Could Mobile Voting Play a Role in the Upcoming Election*, PROTOCOL (Apr. 20, 2020), https://www.protocol.com/sheila-nix-mobile-voting-2020 [https://perma.cc/W8T2-ABMN] (relating an interview with Shelia Nix).

[65] Halpern, *supra* note 63.

[66] *Tusk Philanthropies: Mobile Voting Project*, https://mobilevoting.org/keeping-votes-secure/ [https://perma.cc/8TET-G9US].

[67] Kate Polit, *West Virginia Ditches Controversial Voatz App for May Election*, MERITALK (Mar. 5, 2020), https://www.meritalk.com/articles/west-virginia-ditches-controversial-voatz-app-for-may-election/ [https://perma.cc/LXU5-YDH8]; Voting *Tech Today*, DEMOCRACY LIVE, https://democracylive.com/voting-tech-today-blog/ [https://perma.cc/7NXL-EM6X].

[68] *KCD Board Supervisor Election*, KING CONSERVATION DISTRICT (2020), https://kingcd.org/about/board-of-supervisors/elections-and-appointments/ [https://perma.cc/B9E9-57CM].

administrator and printed for tabulation."[69] Therefore, a "voter verified paper ballot is always available for a hand recount if necessary." Like Voatz, the "voter verified" claim is misleading, since it is impossible for the voter to verify the downloaded ballot that she never even seen.

Democracy Live has not provided security-related details to independent cybersecurity experts. They claim that an "independent audit" by the nonprofit National Cybersecurity Center (NCC) found that the King County election was accurately tabulated and that there was no interference.[70] But no report was publicly released. Moreover, while the CEOs of both Voatz and Democracy Live are on the NCC's Secure the Vote Advisory Board, there is a notable absence of election security experts on the Security Board.[71] Vendor involvement raises questions about the independence of the NCC.

Despite Democracy Live's secrecy, in June 2020 a security analysis of Democracy Live's online voting system was released. [72] The analysis showed that the system was "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 appears to have no privacy policy, 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."[73]

Because of the lack of openness on the part of Democracy Live, the researchers were able to analyze only the application software used by the

---

[69] KING CONSERVATION DIST., FAQ: CAN YOU EXPLAIN HOW OMNIBALLOT IS SECURE?, https://kingcd.org/wp-content/uploads/2020/02/OmniBallot-FAQ-KCD.pdf [https://perma.cc/K3FU-N5ML].

[70] Alyssa Newcomb, *A Mobile, Online Voting Effort Doubled Turnout Last Month Outside Seattle, Independent Audit Says*, FORTUNE (Mar. 5, 2020), https://fortune.com/2020/03/05/mobile-online-voting-seattle-king-county-turnout/ [https://perma.cc/WTK3-XYDD].

[71] Press Release, National Cybersecurity Center, National Cybersecurity Center's Secure the Vote Launches Advisory Board (March 30, 2020), https://cyber-center.org/national-cybersecurity-centers-secure-the-vote-launches-advisory-board/ [https://perma.cc/UQK8-9N9L].

[72] MICHAEL A. SPECTOR & ALEX HALDERMAN, SECURITY ANALYSIS OF THE DEMOCRACY LIVE ONLINE VOTING SYSTEM (Internet Pol'y Res. Initiative, Mass. Inst. Tech., June 7, 2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf [https://perma.cc/R7K7-E86H].

[73] *Id.* at 1. A week after Spector and Halderman published their report, Democracy Live (finally) posted a privacy policy. *See Privacy Policy*, DEMOCRACY LIVE (last updated June 15, 2020, 8:00 A.M.), https://democracylive.com/privacy-policy/ [https://perma.cc/X8WP-LNXZ]. But Democracy Live still collects the voter's name, physical address, email address, telephone number, partial social security number, and information about the phone or computer used to access the site.

voters, and not the software that runs the backend servers.[74] Not long after the security report was released, Delaware initially decided not to use the Democracy Live system for their July 7 primary.[75] Delaware subsequently backtracked by allowing the use of the Democracy Live system coupled with the return of voted ballots via mail, fax, or email, disallowing only casting a voted ballot via the website. The Delaware Department of Elections wrongly claimed that "no votes are cast online under any circumstances".[76] We note that email voting, which has risks similar to website voting, involves sending voted ballots over the Internet, and faxes typically are sent unencrypted, often over the Internet.

VIII. CONCLUSION

The warnings of attacks on our elections have not ceased, with the Department of Homeland Security sounding the alarm: "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions."[77] More than ever, we cannot afford to put our democracy at risk by indulging in Internet voting, especially since there are far safer options.

The burden of proof to show that any Internet voting system is safe should be the responsibility of whoever is advocating for such a system, including policy makers, citizens, and vendors. Until we are provided with such proof, Internet voting—including blockchain voting—should not be deployed in any governmental election.

---

[74] Kim Zetter, *Online Voting System Used in Florida and Elsewhere Has Severe Security Flaws, Researchers Find*, ONEZERO (June 8, 2020), https://onezero.medium.com/researchers-find-security-flaws-in-online-voting-system-used-in-florida-and-other-states-d079ca2af050 [https://perma.cc/54SB-2HWL].

[75] Benjamin Freed, *Delaware Backs Out of Mobile Voting Weeks Before Primary*, STATE SCOOP (June 18, 2020), https://statescoop.com/delaware-backs-out-of-mobile-voting-weeks-before-primary/ [https://perma.cc/X5ZT-RKZZ].

[76] *See* SPECTER & HALDERMAN, *supra* note 72, at 21 (Figure 4).

[77] Press Release, Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections (Nov. 5, 2019), https://www.dhs.gov/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020-elections [https://perma.cc/2XN5-V52H].