Internet Voting is Being Pushed by False Claims and Deceptive Marketing

Susan Greenhalgh[1] [0000-0002-2453-8572]

[1]Free Speech For People, Amherst MA 01002, USA

Abstract.

While the convenience of voting from a computer or smartphone over the Internet may seem to be desirable, there is overwhelming evidence that ballots cast electronically cannot be adequately secured to protect the legitimacy of the votes and integrity of our elections. Despite these conclusion, online voting has only increased in the U.S. This begs the question, why?

From public statements, news reports, press releases and marketing materials it becomes evident that the vendors of these online voting systems have been selling their systems to state and local officials with potentially false, misleading and/or deceptive marketing claims. These spurious claims have served to counter the scientific conclusion that online voting is dangerously insecure and unsuitable for public elections. Moreover, these specious assertions promising security have led state and local government officials to believe, incorrectly, that online voting can be secured, and for these officials to support or press for legislation to adopt and/or expand online voting.

This paper examines spurious or false claims made by the two most prominent Internet voting system vendors in the United States, and the impact these false claims have had on laws and policies to adopt online voting.

Keywords: Internet voting, online voting, cybersecurity.

1 Introduction

While the convenience of voting from a computer or smartphone over the Internet may seem to be desirable, there is overwhelming evidence that ballots cast electronically cannot be adequately secured to protect the legitimacy of the votes and integrity of our elections. There is undisputed, settled science that voted ballots transmitted over the Internet are highly vulnerable to manipulation and privacy risks through a variety of attack vectors, and should not be adopted for public elections. [1]

These cyber risks are intensified by the fact that state-sponsored hackers are actively targeting western democratic election systems to disrupt and/or tamper with elections. Following reports of Russian election interference in 2016, two European nations that had adopted online voting, France [2] and Norway [3], suspended the practice. In April 2020, the U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Institute of Standards and Technology (NIST) and U.S.

Election Assistance Commission (EAC) issued a risk assessment to U.S state election officials which concurred with previous research and academic consensus. The federal agencies risk assessment stated explicitly that online transmission of voted ballots is at high risk of manipulation, even with security controls in place, and that paper balloting is recommended. [4]

Despite these facts, online voting has only increased in the U.S. This begs the question, why?

From public statements, news reports, press releases and marketing materials it becomes evident that the vendors of these online voting systems have been pitching their systems to state and local officials with potentially false, misleading and/or deceptive marketing claims. These spurious claims have served to counter the scientific conclusion that online voting is dangerously insecure and unsuitable for public elections. Moreover, these specious assertions of security have led state and local government officials to believe, incorrectly, that online voting can be secured, and for these officials to press for the adoption and expansion of online voting.

This paper1 examines specious or false claims made by the two most prominent Internet voting system vendors in the United States, and the impact these false claims have had on laws and policies to adopt online voting.

2 Democracy Live

Democracy Live is a Seattle-based company that sells systems that provide electronic blank ballot delivery systems2, remote accessible ballot marking systems3, and full internet voting systems. Democracy Live is aggressively marketing its OmniBallot voting system configured to enable voters to cast and return a ballot online from their own computerized devices.

False Claims of Security

There is widespread consensus from computer scientists and national security experts that any online transmission of voted ballots cannot be secured. [6] In the risk assessment distributed by the DHS, FBI, EAC and NIST, the federal agencies warned, “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.” [3]

[1] This paper was updated in September 2022.

[2] Electronic blank ballot delivery allows a voter to access an electronic image of their ballot that can be printed by the voter, marked with a pen, and returned by mail or drop box.

[3] Remote accessible ballot marking systems allow a voter to access a ballot on her own computer, use accessible technology to make selections on the ballot and print the ballot to be returned by mail or drop box. Remote accessible ballot marking systems can be designed to retain all vote selection data on the voter’s computer, or to transmit the vote choices over the internet, back to a remote server even if the voter prints the ballot and physically returns the printed ballot. [5]

Yet, Democracy Live has maintained in marketing materials for its online ballot return system “OmniBallot,” that ballots transmitted over the Internet through its portal are secure, claiming:

- “OmniBallot is an electronic method of delivering and **returning ballots via a secure online portal**.”
- “OmniBallot offers **secure,** accessible remote balloting for all voters.”
- “OmniBallot utilizes AWS Object Lock to **ensure immutable document (ballot) storage**.”
- “The voter’s ballot selections are encrypted and **securely stored**.”
- “**Accurate** and efficient ballot delivery”
- “**Securely** delivering the correct ballot and ballot materials to eligible voters.”
- “…voters with disabilities and remote voters, can **securely** access and return their ballots in a **more secure** and accessible method.” [7]

Democracy Live has repeated brazen, baseless claims that its online ballot delivery and return system is secure in order to sell its product despite unanimous expert consensus to the contrary.

But more importantly, researchers at the University of Michigan and the Massachusetts Institute of Technology conducted an independent security review of Democracy Live’s OmniBallot online ballot return system and found that it is “vulnerable to vote manipulation by malware on the voter’s device and by insiders or other attackers.” The security researchers went on to warn, “if at all possible, do not return your ballot through OmniBallot’s website or by email or fax. These return modes cause your vote to be transmitted over the Internet, or via networks attached to the Internet, exposing the election to a critical risk that votes will be changed, at wide scale, without detection.” [9]

Any notion that Democracy Live’s claims of security may be founded in well-meaning naivete evaporates when considered alongside Democracy Live’s cynically crafted legal policies and sales contracts which plainly acknowledge that they cannot warrant the accuracy or reliability of the Democracy Live system.

“7.2 democracy live does not represent or warrant that omniballot online will operate error-free or uninterrupted and that all program errors in 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.” [10]

This clause shows that Democracy Live is fully aware of this fact and leverages it to avoid legal liabilities, while simultaneously making untrue marketing claims that it can secure ballots sent over the Internet.

False Claim Regarding Federal Certification of OmniBallot Tablet[4]

Democracy Live's misleading and untrue statements are not limited to claims regarding the security of its online systems. In a press release issued November 2019, Democracy Live wrote:

> "*Seattle-based Democracy Live has been awarded full certification of the first stand-alone accessible balloting device in the elections industry... The OmniBallot Tablet is the first vendor-neutral, off-the-shelf ballot marking device that has been reviewed and approved by an EAC-approved independent test lab.*" [11]

By claiming the device received "full certification," by an "EAC-approved test lab," the press release appears to boast that the OmniBallot Tablet was awarded federal certification by the EAC. However, no OmniBallot product has ever been granted EAC certification. [12] Democracy Live is not even a registered manufacturer of the EAC's testing and certification program, a pre-requisite for any voting system vendor that wishes to pursue EAC certification. [13]

Distorting Perception of Its Systems

Democracy Live has also tried to mute public opposition to its online voting system by falsely recasting the system to election officials and voters as something other than online or Internet voting. In an interview with NPR, Democracy Live CEO Brian Finney admitted "online voting" is "a loaded term" and claimed its system is instead a "document storage application." [14] This directly contradicts the EAC, the National Academies of Science, Engineering and Medicine, [1] and multiple other credible, relevant entities that define Internet or online voting as any process which transmits a voted ballot over the Internet. [15]

Democracy Live has taken this disinformation even further by falsely claiming that its system provides a "voter-verified paper ballot," which is widely viewed as the gold-standard for secure, auditable voting systems. It is true that ballots transmitted over the Internet by Democracy Live are routinely printed at the election office and counted by scanner. However, a paper ballot printed at the election office is not ever viewed or verified by the voter and is plainly not a "voter-verified paper ballot." Yet, in its marketing materials, Democracy Live has claimed, "[s]erving over 600 jurisdictions in the U.S., the OmniBallot portal has generated a voter-verified paper ballot in 100% of all elections." [16]

Democracy Live has repeated this distortion in public statements, press interviews and marketing materials in an attempt to rebrand its product as a paper-based voting system.

Democracy Live's CEO told a local Seattle news outlet:

[4] This section of the report was updated November 3, 2021 to more precisely reflect the fact that the referenced press release related to OmniBallot Tablet.

“*This is really a paper-based document transmission system…At the end of the day, there’s going to be a paper ballot involved. It’s simply storing a document — in this case that document happens to be a ballot — in a federally approved cloud environment.*” [17]

Accessible Voting that is Inaccessible

Democracy Live promotes its system as a solution to provide accessible, absentee voting to voters with disabilities that are unable to handle a paper absentee ballot, like those with visual impairments or manually dexterity issues. Democracy Live has claimed its system is fully accessible for voters with disabilities [18], and meets all accessibility requirements [19],

“*OmniBallot is a fully ADA Section 508, WCAG 2.0aa compliant remote ballot marking solution. The system has been tested to meet the accessibility requirements of over 90 combinations of browsers, operating systems, screen readers and devices. OmniBallot has been deployed as an accessible absentee tool since 2009 and has been tested and reviewed by members of most every leading disability organization in the nation.*” [7]

In January 2020, Democracy Live was engaged to run the Conservation District elections for King County, Washington, boasting that the system would provide accessible ballots to voters with disabilities. [18]

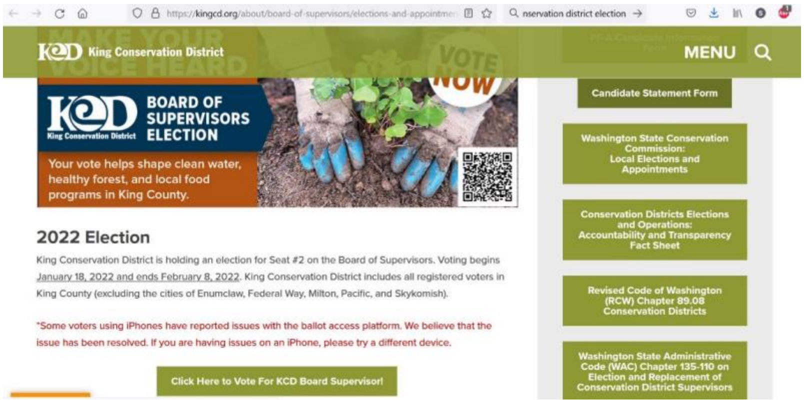
But when it launched in 2020, the Democracy Live system was found to be incompatible with standard accessible screen readers, leaving voters with visual impairments, reliant on screen readers, few options to vote. In response to the undeniable failure, Democracy Live offered voters with disabilities free rides to a local polling place to cast a ballot on an accessible device.

According to a bulletin posted on the King County website:

“*The current mobile voting solution being offered in the King Conservation District election allows voters with disabilities to access, mark, sign and return their ballot entirely independently. However, for vision impaired voters utilizing screen readers, voters must turn off screen readers to sign their name, before turning it back to submit their ballot.*

The issue, which was identified by Disability Rights WA, a local non-profit that protects the rights of people with disabilities statewide, is the result of screen reader incompatibility with Apple and Google operating systems. In order to provide an accessibility option for voters who are not able to turn off their screen reader to sign their ballot and screen, KCD will provide accessible voting locations at their office on Election Day, February 11th from 9:00am through 8:00pm. Free transportation to KCD’s office will be provided for those effected [sic] by the screen reader issue through Democracy Live’s ride-share service. Voters effected by the issue can call 855-655-

VOTE (8683) to arrange transportation to KCD's office, or for questions and assistance with voting from home." [20]



https://kingcd.org/about/board-of-supervisors/elections-and-appointmen
nservation district election
King Conservation District
MENU
VOTE NOW
BOARD OF SUPERVISORS ELECTION
King Conservation District
Candidate Statement Form
Washington State Conservation Commission: Local Elections and Appointments
Conservation Districts Elections and Operations: Accountability and Transparency Fact Sheet
Revised Code of Washington (RCW) Chapter 89.08 Conservation Districts
Washington State Administrative Code (WAC) Chapter 135-110 on Election and Replacement of Conservation District Supervisors
Click Here to Vote For KCD Board Supervisor!

Your vote helps shape clean water, healthy forest, and local food programs in King County.

2022 Election

King Conservation District is holding an election for Seat #2 on the Board of Supervisors. Voting begins January 18, 2022 and ends February 8, 2022. King Conservation District includes all registered voters in King County (excluding the cities of Enumclaw, Federal Way, Milton, Pacific, and Skykomish).

*Some voters using iPhones have reported issues with the ballot access platform. We believe that the issue has been resolved. If you are having issues on an iPhone, please try a different device.

Fig. 1. Two years later, in the 2022 elections, voters were still experiencing issues with the Democracy Live ballot access platform on iPhones, according to a website announcement. In the 2022 election, disabled voters were given no additional options to vote.

The failure of Democracy Live's online voting system to provide ballot access for voters with disabilities was consequential. At a hearing this year of the Washington State legislature, an elected King County Conservation District member testified a constituent with a visual impairment told her she "simply gave up when she was trying to vote, and said, quote, "*It doesn't feel like they even want us to vote*." [21]

3 Voatz

Voatz is a Boston-based startup company that is developing and aggressively marketing an Internet-based voting system that employs a blockchain to enable voters to cast a ballot from an application loaded on to their mobile phones. Voatz' system has been used in municipal elections in Salt Lake City, Utah [22], West Virginia [23] and Denver, Colorado [24].

False Claims of Security

Voatz' campaign to promote its voting system has included bogus claims of "military grade security," [25] public statements asserting that votes cast on its platform could not be deleted or altered, [26] and published materials and presentations [27] promising that Voatz' system was robustly vetted and secure [28]. Though many computer security experts vociferously expressed skepticism or distrust at Voatz' claims as unsupported, spurious or misleading [29], [30] West Virginia elected to engage Voatz to offer its mobile voting system.

In a press release issued by the office of the Secretary of State, Secretary Mac Warner praised Voatz, saying he was pleased with the system. [23] Warner's support for Voatz and confidence in its security was repeated in multiple news stories and in presentations to other election officials. [31] Warner's general counsel Donald Kersey praised the system to a group of Secretaries of State and State election directors, and affirmed that his office was confident the system was trustworthy because of a purported security assessment. [32] In response to an op-ed criticizing Voatz' security and lack of transparency, Secretary Warner authored an op-ed that vigorously defended Voatz and attacked the criticisms as inaccurate. [33] Warner even tried to discredit the criticism by suggesting that opposition to Voatz' online voting system was motivated by a desire to hinder voting by members of the military. Warner's aggressive defense of Voatz' security indicates Voatz' campaign to persuade West Virginia election officials that its system is secure was fruitful.

West Virginia's support of Voatz served to validate the system to other election officials and helped Voatz sell its product in other states. [34] Warner's trust in Voatz' system also drove his efforts to have the legislature pass SB 94 which expands online voting to all West Virginia voters with disabilities. [35]

Similarly, Voatz' technology was actively promoted in Denver, Colorado, which adopted the system for municipal elections. Colorado election officials expressed confidence in Voatz and its security, echoing the false claims in Voatz' marketing materials. Denver County deputy director of elections Jocelyn Bucaro praised Voatz, saying "[w]e are very excited about the promise of this technology. Our goal was to offer a more convenient and secure method for military and overseas citizen voters to cast their ballots, and this pilot proved to be successful." [36]

These statements prove the campaign to persuade election officials that Voatz' system is secure was successful, resulting in an expansion of online voting.

Though Voatz had succeeded in hoodwinking several key election administrators, its failure to substantiate its security claims continued to breed distrust among others. In November 2019, U.S. Senator Ron Wyden (OR) sent a request to the Department of Defense and the National Security Agency asking both to conduct a security evaluation of Voatz, writing:

> "*While Voatz claims to have hired independent security experts to audit the company, its servers and its app, it has yet to publish or release the results of those audits or any other cybersecurity assessments. In fact, Voatz won't even identify its auditors. This level of secrecy hardly inspires confidence*." [37]

In February of 2020, election officials and the public had their first look at Voatz' security from an independent third party when researchers at the Massachusetts Institute of Technology (MIT) published a report that contradicted many of Voatz' claims. The report was a stunning catalogue of security gaps, and documented multiple vulnerabilities "that allow different kinds of adversaries to alter, stop, or expose a user's vote."

By reverse engineering the publicly available Voatz mobile application, the MIT researchers were able to analyze and identify several opportunities to compromise, corrupt or alter votes cast over the Voatz application before the ballot even enters the blockchain. The MIT researchers were able to circumvent Voatz' malware protections with "minimal effort," allowing an attacker to corrupt the Voatz application and undetectably alter or spy on vote choices. The researchers also found that votes cast on the application are not loaded directly onto the blockchain; instead, they first pass through a server which is also vulnerable to multiple attacks that could manipulate or delete votes before they even reach the blockchain, making any public audit of votes recorded on the blockchain meaningless.

In addition to documenting multiple, significant vulnerabilities with the Voatz mobile voting system, the MIT researchers included in the appendices a catalogue of eleven of Voatz' published security claims, annotated by the researchers with findings from their research demonstrating the falsity of Voatz' security representations. [38]

Concerned the vulnerabilities could have national security implications, the MIT researchers reached out to the Cybersecurity Infrastructure and Security Agency (CISA) at DHS to share their findings. CISA found the research credible and facilitated communication between the researchers and Voatz to responsibly disclose the security issues to Voatz before the report was made public. CISA also arranged calls between the MIT researchers and several affected election officials to alert them to the findings.

Voatz responded to the MIT researchers' findings forcefully; staunchly denying their conclusions and vigorously criticizing the research methods on its blog, and on a media call held on the same day the report was made public. Voatz called the research "flawed" [39] and "riddled with holes" as its officers claimed the attacks MIT identified were impossible. [40]

Even though the DHS had validated MIT's findings, Voatz' strenuous denials and attacks on the MIT report succeeded in convincing some of its customers that Voatz' security claims were valid and that the MIT findings were false. Utah County Clerk Amelia Powers Gardner repeated the same spurious explanations Voatz had provided to reporters when justifying the continued use of the application and told reporters there was no evidence the researchers' findings raised security concerns. [41]

A month after the MIT study was published, the independent security firm Trail of Bits (TOB) released a security review it conducted of the Voatz mobile voting platform on behalf of Tusk Philanthropies and Voatz. The Trail of Bits' study was a searing indictment of Voatz' security, affirming all of the assertions made by the MIT team and identifying additional security vulnerabilities in the system. Further, the Trail of Bits study exposes many of the public statements Voatz made in response to the MIT study as false, misleading or specious. According to the Trail of Bits report, TOB confirmed to Voatz all the security vulnerabilities identified by MIT on February 11 two days before Voatz published its denial of the MIT study and held a press call falsely excoriating the MIT report. [42]

Voatz Misleading and Potentially Illegal Use of the DHS Seal and CISA Logo

In September and October of 2019, at Voatz' request, the Hunt and Incident Response Team (HIRT) of DHS's CISA conducted an assessment of Voatz' systems to determine if they contained any evidence or artifacts indicating Voatz had suffered an intrusion.

[43] After its completion, the assessment was provided to Voatz only. As is CISA's practice, the assessment was not made public, nor was it classified.

As described above, in February of 2020, as the researchers at MIT were preparing to release their damning security review of Voatz' application, the MIT team alerted CISA to their findings and CISA in turn, facilitated a meeting between the researchers and Voatz. At the meeting, Voatz was made aware not only of the damaging findings, but that they would soon be reported in *The New York Times*.

In mid-February 2020, with a media storm looming, Voatz delivered a summary of HIRT's findings, written by Voatz, to the West Virginia Secretary of State's office. [44]

The Voatz' summary, provided February 11, 2020, prominently displays the DHS seal and CISA logo, as well as the Voatz logo. It contains no disclaimer or mark alerting the reader that the document was not written by DHS or CISA. [45]

Once the MIT report was published by *The New York Times,* a media frenzy ensued and Voatz held a press call to criticize and disavow the researchers' findings. On the press call Voatz' CEO Nimit Sawhney identified the Voatz summary as a DHS security audit, telling reporters:

"…there are some audits happening for which information is publicly available. One of them was conducted by the DHS. That's [sic] report is available on our website…" [40]

As one of the most vocal supporters of Voatz' system the West Virginia Secretary of State's office fielded multiple calls from reporters regarding the MIT report. The Secretary of State shared the falsely labeled summary with several reporters and cited it to counter the damaging revelations in the MIT study. [46] Several media reports then described the summary as a declassified DHS report. [5]

Voatz publicly released an updated version of this report sometime after February 14, 2020, which removed the DHS seal and CISA logo, and added a disclaimer clarifying that Voatz created the summary. **[43]** Voatz' falsely labeled summary may constitute a violation of 18 U.S.C. § 701 (prohibiting use of government insignias except as provided by regulations), [47] or 18 U.S.C. § 1017 (prohibiting false use of government insignias). [48]

Although the currently public version of the summary no longer uses the DHS seal, Voatz may have also used DHS branding on other materials it may have provided to its customers.

It appears the Voatz summary was written and distributed with the government logo to blunt the impact of the MIT report, and maintain the company's standing in the marketplace.

[5] The Mother Jones article continues to link to the original, falsely labeled, Voatz summary. *Id.* ("Warner's office also provided a copy of a declassified DHS assessment of the Voatz network.")

4 Conclusions and Recommendations

As reflected in testimony before the U.S. Congress, regulations on polling place voting machines are woefully insufficient. [49] Online voting systems and vendors are not regulated at all. There is absolutely no oversight, regulation or accountability for the vendors of online voting systems and they appear to have exploited this fact to sell their systems with spurious claims. Moreover, states are adopting policies and passing legislation to expand online voting, supported by the untrue expectation that vendors can supply secure systems.

We recommend the false claims made by these vendors be fully investigated by relevant authorities including: the Federal Trade Commission, the Department of Justice, State Attorneys General and relevant Congressional Committees. We must not permit the vendors' self-interested, untrue marketing strategies promote election policies and legislation that put our elections at risk.

Acknowledgements. Free Speech For People would like to thank Dr. Michael Spector and Professor J. Alex Halderman, whose research provided facts central to this report, and whose input was essential. We would also like to thank Ron Fein, Travis Arbor, Sarah Fender, and Zakary Kaddish for their contributions. Finally, we would like to thank Craig Newmark and Craig Newmark Philanthropies, and Marion Edy and the Threshold Foundation for making this report possible.

5 References

1. Securing the Vote, Protecting American Democracy, National Academies of Science, Engineering and Medicine. (2018). *https://www.nap.edu/read/25120/chapter/1*
2. France Drops Electronic Voting for Citizens Living Abroad Over Cyber Security Fears. Reuters. (2017). https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233.
3. Amundson, B.: No more online voting in Norway. Science Norway. (2019). https://sciencenorway.no/election-politics-technology/no-more-online-voting-in-norway/1562253
4. Risk Management For Electronic Ballot Delivery, Marking, and Return. U.S. Election Assistance Commission, National Institute of Standards and Technology, Federal Bureau of Investigation, Cybersecurity Infrastructure Security Agency. (2020). https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mod=article_
5. Greenhalgh, S., Newell S.: Leveraging Electronic Balloting Options Safely and Securely During the COVID-19 Pandemic. Free Speech For People and American Association for the Advancement of Science. (2020). https://freespeechforpeople.org/wp-content/uploads/2020/06/rabm.white_.paper_.6.23.20.pdf
6. Letter to Governors and Secretaries of State on the insecurity of online voting. AAAS Center for Scientific Evidence in Public Issues. (2020). https://www.aaas.org/programs/epi-center/internet-voting-letter

7. Omniballot Fact Sheet. https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf (emphasis added).
8. Gutman, D.: Online voting is coming to Seattle, but only for an election you've likely never heard of. Seattle Times. (2020) https://www.seattletimes.com/seattle-news/politics/online-mobile-voting-is-coming-to-king-county-but-only-for-an-election-youve-likely-never-heard-of/
9. Spector, M, Halderman, J. Alex.: Security Analysis of the Democracy Live Online Voting System, University of Michigan. (2020). https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf
10. Contract between Democracy Live and Williamson County, TX. Page 3. https://agenda.wilco.org/docs/2020/COM/20200107_1503/23436_Williamson%20County%20UOCAVA%20Agreement%20revised%2012.17.19.pdf
11. Democracy Live Awarded Certification Approval for Dell/Windows 10 IoT Enterprise Balloting Solution. BusinessWire, (2019). https://www.businesswire.com/news/home/20191111005677/en/
12. https://www.eac.gov/voting-equipment/certified-voting-systems
13. https://www.eac.gov/voting-equipment/registered-manufacturers
14. Parks, M.: States Expand Internet Voting Experiments Amid Pandemic, Raising Security Fears, NPR (2020). https://www.npr.org/2020/04/28/844581667/states-expand-internet-voting-experiments-amid-pandemic-raising-security-fears
15. U.S. Election Assistance Commission: A survey of Internet voting (2011), https://www.eac.gov/sites/default/files/eac_assets/1/28/SIV-FINAL.pdf
16. https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf
17. Bowman, N.: King County district to use one-of-a-kind smartphone voting platform for third straight year.MyNorthwest. (2022). https://mynorthwest.com/3301713/king-conservation-district-smartphone-voting-2022/
18. Democracy Live Press Release, Mobile Voting is Coming to Voters in King County, WA. (2020). https://www.prnewswire.com/news-releases/mobile-voting-is-coming-to-voters-in-king-county-wa-300990874.html
19. Democracy Live Omniballot Portal, Accessible Remote Balloting Portal flyer. https://democracylive.com/wp-content/uploads/2022/04/OmniBallot-Portal-Democracy-Live_1.17.22.jpg
20. King Conservation District and Democracy Live to Offer Additional Accessible Voting Options. (2020). Available at: King Conservation District and Democracy Live to Offer Additional Accessible Voting Options : King Conservation District (kingcd.org)
21. Testimony of Brittney Bush Bollay, elected member of the King County Conservation District, at the January 27, 2022 House State and Tribal Government Committee hearing of the Washington State legislature. https://tvw.org/video/house-state-government-tribal-relations-committee-2022011573/?eventID=2022011573 at 38:10.
22. Utah County to use voting app despite security concerns. Associated Press. (2020). https://apnews.com/article/0efd3ae8988bf3cf222329400119f1cf
23. Warner Pleased with Participation in Test Pilot for Mobile Voting.: Secretary of State Mac Warner. (2018). https://sos.wv.gov/news/Pages/11-16-2018-A.aspx

24. Kenney, A.: Denver will allow smartphone voting for thousands of people (but probably not you). Denver Post. (2019). https://www.denverpost.com/2019/03/07/voting-smartphone-blockchain-denver
25. Voatz.: Military-Grade Security, Easy To Use: Elections Technology & Civic Engagement. https://freespeechforpeople.org/wp-content/uploads/2020/04/Voatz_1Pager.military.grade_.pdf
26. Hackett, R.: Denver and West Virginia Deserve Praise for Voting on Blockchain. Fortune. (2019). https://fortune.com/2019/03/23/blockchain-vote-election-denver-west-virginia-voatz/
27. https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf
28. Voatz.: Frequently Asked Questions. https://www.voatz.com/faq.html
29. Kosoff, M.: A Horrifically Bad Idea: Smartphone Voting is Coming Just in Time for the Midterms. Vanity Fair. (2018). https://www.vanityfair.com/news/2018/08/smartphone-voting-is-coming-just-in-time-for-midterms-voatz
30. Jefferson, D.et al.: What We Don't Know About the Voatz "Blockchain" Internet Voting System. (2019). https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf
31. Mistich, D.: New Study Says West Virginia's Mobile Voting Pilot Increased Turnout, Notes Security Concerns. West Virginia Public Broadcasting. (2019). https://www.wvpublic.org/post/new-study-says-west-virginia-s-mobile-voting-pilot-increased-turnout-notes-security-concerns#stream/0
32. Freed, B.: West Virginia may offer blockchain-based ballots to all of its overseas voters this November. StateScoop (2018). https://statescoop.com/west-virginia-may-offer-blockchain-based-ballots-to-all-of-its-overseas-voters-this-november/
33. Warner, M.: Criticism of mobile voting project were misinformed, suspect. Charleston Gazette-Mail. (2018). https://www.wvgazettemail.com/opinion/op_ed_commentaries/mac-warner-criticism-of-military-mobile-voting-project-were-misinformed/article_7757947f-693d-5229-bce5-331e7ff35cb0.html
34. Sylte, A.: Need to cast a ballot from overseas? Denver now has an app for that 9News. (2019). https://www.9news.com/article/news/local/next/need-to-cast-a-ballot-from-overseas-denver-now-has-an-app-for-that/73-66118959-c135-4bdb-814d-a2233dc7c427
35. West Virginia pushes online voting for the disabled. GCN. (2020). https://gcn.com/articles/2020/02/03/west-virginia-mobile-voting-disabled-persons.aspx
36. National Cybersecurity Center Successfully Completes Third Party Audit for Denver's Mobile Voting Pilot. PRNewswire. (2019). https://www.prnewswire.com/news-releases/national-cybersecurity-center-successfully-completes-third-party-security-audit-for-denvers-mobile-voting-pilot-300896234.html
37. https://www.washingtonpost.com/context/sen-ron-wyden-d-ore-letter-regarding-voatz/e9e6dd4f-1752-4c46-8e37-08a0f21dd042/
38. Spector, M. et al: The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Massachusetts Institute of Technology.(2020).
39. https://blog.voatz.com/?p=1209

40. Voatz Open Press Call Transcribed from February 13, 2020. https://blog.voatz.com/?p=1243
41. Utah County to use voting app despite security concerns. Utah Public Radio. (2020). https://www.upr.org/utah-news/2020-02-19/utah-county-to-use-voting-app-despite-security-concerns
42. Our Full Report on the Voatz Mobile Voting Platform. Trail of Bits. (2020). https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/
43. Voatz, Hunt Engagement Summary. https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf (2020).
44. Donald Kersey, General Counsel to West Virginia Secretary of State, email to Susan Greenhalgh. Available at: https://bit.ly/3wEMDca
45. Initial Voatz Hunt Assessment Summary. https://bit.ly/3uqefAw
46. Vicens, AJ.: Security Researchers Find Flaws in Online Voting System Tested in Five States. Mother Jones (2020), https://bit.ly/3dcuQjq
47. 18 U.S.C. § 701 (official badges, identification cards, other insignia).
48. 18 U.S.C. § 1017 (government seals wrongfully used and instruments wrongfully sealed).
49. Testimony of Lawrence Norden. Election Security. Committee on House Administration, May 8, 2019. https://www.brennancenter.org/sites/default/files/analysis/Lawrence%20Norden%202019%20Congressional%20Testimony%20on%20Election%20Security.pdf