Internet Voting is Being Pushed by False Claims and Deceptive Marketing

June 2021

Susan Greenhalgh, Senior Advisor on Election Security
Free Speech For People

FREE SPEECH FOR PEOPLE .ORG

ABOUT THE AUTHOR

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from *The New York Times, The Washington Post, The Wall Street Journal, Politico, USA Today, Associated Press, National Public Radio* and other leading news outlets. She has appeared on CNN and MSNBC's *The Rachel Maddow Show,* and various other television and radio news shows. She has a BA in Chemistry from the University of Vermont.

ABOUT FREE SPEECH FOR PEOPLE

Free Speech For People works to renew our democracy and our United States Constitution for we the people. Founded on the day of the Supreme Court's *Citizens United* ruling, Free Speech For People envisions a democratic process in which all people have an equal voice and an equal vote. We fight for free and fair elections, for reliable and secure voting systems, and for the bedrock principle that, in a democracy, all voters must have their votes properly counted. To learn more, please visit our website: www.freespeechforpeople.org.

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.

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 increase 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 paper 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.

DEMOCRACY LIVE

Democracy Live is a Seattle-based company that sells systems that provide electronic blank ballot delivery systems,[5] remote accessible ballot marking systems,[6] 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.[7] 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."[8]

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**."[9]
- "OmniBallot offers **secure,** accessible remote balloting for all voters."[10]
- "OmniBallot utilizes AWS Object Lock to **ensure immutable document (ballot) storage**."[11]
- "The voter's ballot selections are encrypted and **securely stored**."[12]
- "**Accurate** and efficient ballot delivery"[13]
- "**Securely** delivering the correct ballot and ballot materials to eligible voters."[14]
- "…voters with disabilities and remote voters, can **securely** access and return their ballots in a **more secure** and accessible method.[15]

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."[16] 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."[17]

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."*[18]

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

Democracy Live's misleading and untrue statements are not limited to claims regarding the security of its 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."[19]

The press release appears to boast that the OmniBallot tablet was awarded federal certification by the EAC. However, OmniBallot has never been granted EAC certification.[20] 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.[21] These false marketing claims were so egregious that the EAC took the unprecedented step to issue a press release stating directly that the EAC has not certified any online voting system.[22]

DISTORTING PERCEPTION OF ITS SYSTEM

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."[23] This directly contradicts the EAC,[24] the National Academies of Science,

Engineering and Medicine,[25] and multiple other credible, relevant entities that define Internet or online voting as any process which transmits a voted ballot over the Internet.

Democracy Live has taken this disinformation even further by falsely claiming that its system provides a "voter-verified paper ballot,"[26] 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."[27]

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,[28] West Virginia[29] and Denver, Colorado.[30].

FALSE CLAIMS OF SECURITY

Voatz' campaign to promote its voting system has included bogus claims of "military grade security,"[31] public statements asserting that votes cast on its platform could not be deleted or altered,[32] and published materials[33] and presentations[34] promising that Voatz' system was robustly vetted and secure.[35] Though many computer security experts vociferously expressed skepticism or distrust at Voatz' claims as unsupported, spurious or misleading[36],[37] 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.[38] Warner's support for Voatz and confidence in its security was repeated in multiple news stories[39] and in presentations to other election officials. 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.[40] 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.[41] 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.[42] 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.[43]

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."[44]

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."*[45]

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."[46]

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.[47]

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.[48]

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"[49] and "riddled with holes"[50] as its officers claimed the attacks MIT identified were impossible.[51]

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.[52]

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.[53] 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[54] and held a press call falsely excoriating the MIT report.

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.[55] 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.[56]

The Voatz' summary, provided February 11, 2020, prominently displays the DHS seal and CISA logo, as well as the Voatz logo.[57] It contains no disclaimer or mark alerting the reader that the document was not written by DHS or CISA.[58]

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…"[59]

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.[60] Several media reports then described the summary as a declassified DHS report.[61]

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.[62] Voatz' falsely labeled summary may constitute a violation of 18 U.S.C. § 701 (prohibiting use of government insignias except as provided by regulations),[63] or 18 U.S.C. § 1017 (prohibiting false use of government insignias).[64]

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.

CONCLUSION AND RECOMMENDATIONS

As reflected in testimony before the U.S. Congress, regulations on polling place voting machines are woefully insufficient.[65] 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.

Endnotes

[1] "Securing the Vote, Protecting American Democracy," National Academies of Science, Engineering and Medicine. 2018. *Available at: https://www.nap.edu/read/25120/chapter/1*

[2] "France Drops Electronic Voting for Citizens Living Abroad Over Cyber Security Fears," *Reuters* March 6, 2017, https://www.reuters. com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233.

[3] Bard Amundson, "No more online voting in Norway," *Science Norway,* September 12, 2019. *Available at: 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. *Available at:* https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mod=article_inline

[5] 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.

[6] 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. For more information see: Leveraging Electronic Balloting Options Safely and Securely During the COVID-19 Pandemic," Susan Greenhalgh, Dr. Steve Newell, Free Speech For People and American Association for the Advancement of Science, available at: https://freespeechforpeople.org/wp-content/uploads/2020/06/rabm.white_.paper_.6.23.20.pdf

[7] "Letter to Governors and Secretaries of State on the insecurity of online voting," AAAS Center for Scientific Evidence in Public Issues. April 9, 2020. *Available at:* https://www.aaas.org/programs/epi-center/internet-voting-letter

[8] *See supra* note 4.
[9] https://democracylive.com/OmniBallot-online/ (emphasis added).
[10] Ibid. (emphasis added).
[11] Ibid. (emphasis added).
[12] Ibid. (emphasis added).
[13] Ibid. (emphasis added).
[14] Ibid. (emphasis added).
[15] Democracy Live CEO Brian Finney as quoted by David Gutman in "Online, mobile voting is coming to King County – but only for an election you've never heard of," *Seattle Times,* January 22, 2020. *Available at: 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/*(emphasis added).
[16] Michael A. Spector, J. Alex Halderman, Security Analysis of the Democracy Live Online Voting System," University of Michigan, June 7, 2020. *Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf*
[17] Ibid.
[18] Contract between Democracy Live and Williamson County, TX. Page 3. *Available at: https://agenda.wilco.org/docs/2020/COM/20200107_1503/23436_Williamson%20County%20UOCAVA%20Agreement%20revised%2012.17.19.pdf*
[19] "Democracy Live Awarded Certification Approval for Dell/Windows 10 IoT Enterprise Balloting Solution," *BusinessWire,* November 11, 2019. *Available at: https://www.businesswire.com/news/home/20191111005677/en/*
[20] https://www.eac.gov/voting-equipment/certified-voting-systems
[21] https://www.eac.gov/voting-equipment/registered-manufacturers
[22] "U.S. Election Assistance Commission Responds to Recent VVSG-Compliant Testing Claims," *Available at: https://www.eac.gov/news/2020/07/23/us-election-assistance-commission-responds-recent-vvsg-compliant-testing-claims*
[23] Miles Parks, "States Expand Internet Voting Experiments Amid Pandemic, Raising Security Fears," *NPR,* April 28, 2020. *Available at: https://www.npr.org/2020/04/28/844581667/states-expand-internet-voting-experiments-amid-pandemic-raising-security-fears*
[24] U.S. Election Assistance Commission: A survey of Internet voting (2011), https://www.eac.gov/sites/default/_les/eac assets/1/28/SIV-FINAL.pdf
[25] *See supra* note 1.
[26] https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf
[27] Ibid.
[28] "Utah County to use voting app despite security concerns," *Associated Press,* February 18, 2020. *Available at: https://apnews.com/article/0efd3ae8988bf3cf222329400119f1cf*
[29] "Warner Pleased with Participation in Test Pilot for Mobile Voting," Secretary of State Mac Warner, November 16, 2018. *Available at: https://sos.wv.gov/news/Pages/11-16-2018-A.aspx*

[30] Andrew Kenney, "Denver will allow smartphone voting for thousands of people (but probably not you)," *Denver Post,* March 7, 2019. *Available at: https://www.denverpost.com/2019/03/07/voting-smartphone-blockchain-denver/*
[31] Voatz, "Military-Grade Security, Easy To Use: Elections Technology & Civic Engagement," https://freespeechforpeople.org/wp-content/uploads/2020/04/Voatz_1Pager.military.grade_.pdf
[32] Robert Hackett, "Denver and West Virginia Deserve Praise for Voting on Blockchain," *Fortune,* March 23, 2019 https://fortune.com/2019/03/23/blockchain-vote-election-denver-west-virginia-voatz/
[33] https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf
[34] *Ibid.*
[35] Voatz, "Frequently Asked Questions," https://www.voatz.com/faq.html
[36] Maya Kosoff, "A Horrifically Bad Idea: Smartphone Voting is Coming Just in Time for the Midterms," *Vanity Fair,* August 7, 2018
[37] Dr. David Jefferson, et al, "What We Don't Know About the Voatz "Blockchain" Internet Voting System," May 1, 2019, https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf
[38] See *supra* note 29.

[39] Dave Mistich, "New Study Says West Virginia's Mobile Voting Pilot Increased Turnout, Notes Security Concerns," *West Virginia Public Broadcasting,* August 13, 2019. *Available at: https://www.wvpublic.org/post/new-study-says-west-virginia-s-mobile-voting-pilot-increased-turnout-notes-security-concerns#stream/0*
[40] Benjamin Freed, "West Virginia may offer blockchain-based ballots to all of its overseas voters this November," *StateScoop,* July 16, 2018. *Available at: https://statescoop.com/west-virginia-may-offer-blockchain-based-ballots-to-all-of-its-overseas-voters-this-november/*
[41] Mac Warner, "Criticism of mobile voting project were misinformed, suspect," *Charleston Gazette-Mail,* August 12, 2018. *Available at: 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*
[42] Allison Sylte, "Need to cast a ballot from overseas? Denver now has an app for that," *9News,* March 7, 2019. *Available at: 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*
[43] "West Virginia pushes online voting for the disabled," *GCN,* February 3, 2020. *Available at: https://gcn.com/articles/2020/02/03/west-virginia-mobile-voting-disabled-persons.aspx*
[44] National Cybersecurity Center Successfully Completes Third Party Audit for Denver's Mobile Voting Pilot," *PRNewswire,* August 5, 2019. *Available at: https://www.prnewswire.com/news-releases/national-cybersecurity-center-successfully-completes-third-party-security-audit-for-denvers-mobile-voting-pilot-300896234.html*
[45] *Available at*: https://www.washingtonpost.com/context/sen-ron-wyden-d-ore-letter-regarding-voatz/e9e6dd4f-1752-4c46-8e37-08a0f21dd042/
[46] Michael Spector, 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," Massachusetts Institute of Technology, February 2020.
[47] Ibid.
[48] Ibid.
[49] https://blog.voatz.com/?p=1209
[50] https://blog.voatz.com/?p=1243
[51] Ibid.
[52] Connor Richards, "Utah County still plans on using voting app despite security concerns raised by researchers," *Daily Herald,* February 17, 2020. *Available at:* https://www.heraldextra.com/news/local/govt-and-politics/utah-county-still-plans-on-using-voting-app-despite-security/article_ae0d1c54-8b17-5a09-9946-3f3585bda72f.html
[53] "Our Full Report on the Voatz Mobile Voting Platform," Trail of Bits, March 13, 2020. Available at: https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/
[54] Ibid.
[55] Voatz, Hunt Engagement Summary, https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf (Feb. 14, 2020).
[56] Donald Kersey, General Counsel to West Virginia Secretary of State, email to Susan Greenhalgh, available at: https://bit.ly/3wEMDca
[57] Initial Voatz Hunt Assessment Summary, available at: https://bit.ly/3uqefAw
[58] Ibid.
[59] https://blog.voatz.com/?p=1243
[60] AJ Vicens, *Security Researchers Find Flaws in Online Voting System Tested in Five States*, Mother Jones (Feb. 13, 2020), https://bit.ly/3dcuQjq
[61] 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.")
[62] Hunt Engagement Summary, *supra* note 55.
[63] 18 U.S.C. § 701 (official badges, identification cards, other insignia).
[64] 18 U.S.C. § 1017 (government seals wrongfully used and instruments wrongfully sealed).
[65] Testimony of Lawrence Norden, "Election Security," Committee on House Administration, May 8, 2019. *Available at: https://www.brennancenter.org/sites/default/files/analysis/Lawrence%20Norden%202019%20Congressional%20Testimony%20on%20Election%20Security.pdf*