Testimony of Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People
before the
Judiciary Committee
Rhode Island Senate
Contact: susan@freespeechforpeople.org
February 23, 2026
Re: H. 7007 Electronic Ballot Return Extension
OPPOSE

Chair LaMountain, Vice Chair McKenney, and members of the Committee, thank you for the opportunity to submit testimony on H. 7007.

Free Speech For People is a national, non-profit, non-partisan public interest legal organization that works to protect and renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions and advocacy, secure, transparent, trustworthy, and accessible voting policies for all voters. For example, we launched a legal challenge to voter registration restrictions in Arizona, resulting in tens of thousands of additional voters being able to register to vote.

We avidly support the safe use of technology to improve access to the ballot for all voters, particularly underserved voters, and we support the exploration of increased accessible voting options and improvements for voters with disabilities or difficulty accessing a ballot. *But we vigorously oppose the electronic return of voted ballots because ballots transmitted electronically, by email, fax and online ballot portal, are all at high risk for privacy risks, manipulation, and fraud.* At a time when election confidence is under attack, employing dangerously insecure electronic ballot return will degrade not just the security of Rhode Island's elections, but also confidence in elections and trust in government.

We recognized that Rhode Island has permitted military, overseas and voters with disabilities to return ballots electronically through a portal since it passed S.2118 in 2022. We also commend the legislature for prudently including a sunset clause that caused the legislation to expire at the end of last

year, wisely giving Rhode Islanders the opportunity to reassess this policy in light of more recent research and developments.

Specifically, in addition to the numerous research studies that have concluded there are security challenges unique to electronic voted ballot return that cannot be solved with the internet security tools available today and that online ballot return is unacceptably insecure, a study was released from the University of California at Berkeley in 2022 which reaffirmed these findings.[1] This study is notable as it was commissioned by Bradley Tusk, a prominent proponent for online voting.

Rhode Island's online voting system vendor paid for biased "academic research."

In 2023, Cyberscoop published an expose' which revealed that the vendor that has supplied Rhode Island's online voting system, Democracy Live, had paid academics to publish research promoting electronic ballot return.[2] The reporter established that a "research paper" had been drafted with substantial input and editing from Democracy Live's president and founder in order to support Democracy Live's effort to pass state and federal legislation to allow online voting.

The Democracy Live system used in Rhode Island has failed an independent security review.

H. 7007 requires Rhode Island's online voting system to undergo an independent security review, but the legislation does not contemplate what to do if the security review is damning.

The vendor often touts what it represents to be independent security reviews, but these are engagements initiated and designed by the vendor, and which support the adoption of online voting.

In fact, the Democracy Live system *has* undergone a *truly independent* security

[1] R. Michael Alvarez et al., University of California, Berkeley Center for Security in Politics, Working Group Statement on Developing Standards for Internet Ballot Return 10 (2022), https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf.

[2] Yael Grauer, Cyberscoop; *Online voting provider paid for academic research in attempt to sway U.S. lawmakers*; March 29, 2023 (https://cyberscoop.com/democracy-live-research-online-voting/).

review by researchers at the Massachusetts Institute of Technology and the University of Michigan. Contrary to claims by the vendor, the resulting report was peer-reviewed and published by the prestigious USENIX Security Conference. The researchers found the Democracy Live product easily hackable, writing:

"We conclude that using OmniBallot for electronic ballot return represents a severe risk to election security and could allow attackers to alter election results without detection."[3]

Ballots returned online are at high risk for undetectable manipulation or fraud.

Quite plainly, ballots cannot be securely returned electronically**.** Despite assurances from the vendor and the Secretary of State, the system in use in Rhode Island is undeniably at high risk of undetectable tampering and manipulation. Just because no incidents have been reported, this does not prove the system is secure.

Proponents of electronic ballot return may suggest, erroneously, that secure online return of voted ballots is possible with today's computer security tools, or that the use of cloud storage or a portal will adequately protect ballot security. All this is incorrect.

In 2020 and again in 2024, the Department of Homeland Security, the Federal Bureau of Investigation, the National Institute of Standards and Technology and the U.S. Election Assistance Commission published a risk-assessment[4] which "*recommends paper ballot return, as electronic ballot return technologies are high risk even with controls in place*."[5] [Emphasis added.] In other words, the Department of Homeland Security recommends states should continue to use paper ballots because there are serious and significant security risks introduced with the electronic transmission of marked ballots that cannot be adequately mitigated with the security tools and controls available, and ballots returned online are at high risk of tampering or manipulation.

DHS's blunt warning against the use of online voting echoed bipartisan recommendations from the U.S. Senate Select Committee on Intelligence, published in response to findings that foreign governments were actively trying to

[3] 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*

[4] Available at: https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001

[5] *Ibid*.

attack U.S. election systems. The Committee explicitly wrote: "States should resist pushes for online voting."[6]

In 2018, the National Academies of Sciences, Engineering and Medicine (NASEM) released a report stating that the technology to return marked ballots securely and anonymously over the internet does not exist.[7] Many studies have reviewed specific[8] internet[9] voting systems[10] and consistently, all have found that despite their claims of innovation and security, these systems have fundamental vulnerabilities that are not remediable.

At a time when election security and public confidence in our elections are under attack, increased electronic return of voted ballots, whether from a phone, tablet, or computer, is simply not safe or secure in any form.

Online voting is not comparable to online banking.

The public may ask, 'I can bank online, why can't I vote online?' But voting involves critical differences that make it a much more difficult enterprise to secure than online banking or commerce.[11] Online transactions are not secret or anonymous; a customer can check her statement to detect and address fraudulent charges. But we vote by secret ballot; there is no mechanism for the voter or election official to check to ensure ballots were not manipulated or hacked in transit and that the votes are legitimate. This makes online elections especially vulnerable to undetectable hacking.

And even if an attack was detected, there would be no way for election officials to determine which ballots were manipulated and which are legitimate, making an online attack uncorrectable. Such systems are, by definition, not auditable; since

[6] Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 2019*, Available at* *https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf*

[7] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. *Available at: https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy*

[8] Massachusetts Institute of Technology, 2020. "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections." https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

[9] "Our full report on the Voatz Internet voting system," Trail of Bits, March 13, 2020. *Available at:* *https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/*

[10] See *supra* note 3.

[11] "If I Can Shop and Bank Online, Why Can't I Vote Online?" *by David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory, member, Verified Voting Foundation Board, Board of Directors, California Voter Foundation https://www.verifiedvoting.org/resources/internet-voting/vote-online/*

there is no indelible source record of voter intent, there is no audit record. In addition, banks may calculate an acceptable level of fraud and factor that into the cost of doing business, or take out insurance to cover their losses, but we cannot accept any illegitimate ballots. Finally, the assumption that online banking can be done securely is faulty. It is estimated that banks lose millions or even billions of dollars every year to online attacks.[12] High profile hacks like that on Citibank, JP Morgan Chase, and Bank of America prove that even system with high cyber security budgets (much higher than Rhode Island's), cannot resist determined attackers.

Use of online voting is not evidence that it is secure.

Although Rhode Island and other states currently permit electronic ballot return, that does not mean it is secure or trustworthy.

During the early 2000's, Congress tasked the Department of Defense, through the National Defense Authorization Act, to develop a secure online voting system for military voters. Consequently, many states passed laws to permit electronic ballot return, planning to opt into the system provided by the Department of Defense. A system was developed in 2004, but was never deployed because a security evaluation determined that illegitimate ballots could be cast undetectably. Subsequently, after years of federal research that concluded electronic ballot return could not be made secure,[13] the Department of Defense and federal government abandoned the effort.

It's important to also understand that most of these states enacted policies to allow online return of voted ballots when cybercrime was much less commonplace and mature. Cybercrime has advanced significantly in the last decade, and by expert accounts, the expertise and sophistication of today's cyber criminals has far out-paced our defenses. We know much more today than we did then, and today's policy decisions should be based on the current threat model.

Alternative accessible voting options should be explored.

[12] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[13] https://www.nist.gov/itl/voting/uocava-voting

At present, voters with disabilities still experience significant barriers to casting their votes privately and securely,[14] and we should make efforts to resolve these challenges. We understand the profound difficulties you face to assure every voter's ability to vote and strongly support interventions to assure voters' equal opportunity and access to cast their vote – securely and verifiably. Recognizing that no current solution is ideal for all voters, we support thoughtful consideration to improve secure innovations, such as mobile accessible voting. Mobile accessible voting is offered in some states where election workers bring accessible ballot marking devices to the residences and workplaces of voters with disabilities. These accessible devices allow disabled voters to privately and independently cast a secured, verifiable paper ballot with accessible technology. (Currently Oregon and San Francisco and its neighboring counties have launched such an effort.[15])

We would welcome the opportunity to provide the Committee with further information on technical aspects of electronic ballot return. We urge the Committee to reject H.7007 and allow this practice to sunset in Rhode Island.

Thank you for your consideration.

Susan Greenhalgh
Senior Advisor for Election Security

Free Speech For People

[14] "Disability and Voting Accessibility in the 2020 Elections, Final Report on Survey Results." February 16, 2021. Rutgers University; U.S. Election Assistance Commission. *Available at: https://smlr.rutgers.edu/sites/default/files/Documents/Centers/Program_Disability_Research/Disability_and_voting_accessibility_2020_election_Final_Report_survey_results.pdf*

[15] San Francisco, Oakland, San Jose and some of the twelve counties that surround it have invested a $1 million federal grant to provide Mobile Voting Vehicles to increase voting access to disabled and underserved voters. See: http://www.bayareauasi.org/sites/default/files/resources/approval_2022_january_meeting_master.pdf, page 57.