Berkeley
Public Policy
The Goldman School

University of California, Berkeley
Center for Security in Politics

December | 2022

Working Group Statement on Developing Standards for Internet Ballot Return

CENTER FOR SECURITY IN POLITICS
UNIVERSITY OF CALIFORNIA, BERKELEY

Authors

R. Michael Alvarez, Professor of Political and Computational Social Science, California Institute of Technology
Mike Garcia, Cybersecurity and Election Security Expert
Josh Benaloh, Microsoft Research
Roy Herrera, Partner, Herrera Arellano LLP
Allie Bones, Assistant Secretary of State, Arizona
Henry E. Brady, Director of Research, California 100
Amber McReynolds, National Election Expert & Former Election Official
Jeremy Epstein, Chair, Association for Computing Machinery U.S. Technology Policy Committee
Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology
Anthony Fowler, Professor, University of Chicago
Maurice Turner, Public Interest Technologist
Michael J. Frias, Chief Executive Officer, Catalist
Mark Weatherford, Chief Security Officer, AlertEnterprise

Table of Contents

Introduction

Americans conduct an ever-increasing amount of personal business over the internet, from banking to healthcare to real estate purchases. Yet, except for a few limited circumstances such as some voters with accessibility needs, internet voting has not been adopted as common in U.S. public elections.

Accordingly, in August of 2021 through September of 2022, the University of California Berkeley's Center for Security in Politics (CSP), through funding provided by Tusk Philanthropies, hosted a Working Group to determine the feasibility of technical and implementation standards that would enable safe and secure digital remote ballot marking and return of these ballots.

The Working Group will refer to "internet ballot return" throughout this statement. This term is inclusive of marking a ballot remotely, particularly through a voter's personal device, and returning the ballot via the internet. Internet ballot return includes, but is not limited to, use of browsers, apps, email, file transfer protocol, and facsimile.

Election officials must balance fairness, accessibility, security, transparency, equity, and reliability when delivering solutions for voters. And they are doing so in a time of extreme scrutiny and skepticism about well-established, long-standing, and reliable elections practices. The use of technology is being questioned for processes that have been in place for decades (e.g., tabulation of ballots), so introducing new technologies into elections administration will take careful thought, consideration, and planning, along with increased capacity and resources for election officials currently under intense pressure amid staff turnover, record numbers of public records requests, and physical threats of violence for doing their jobs. It is in this context that the Working Group provides this statement.

Conclusions

The Working Group has four major conclusions:

1. **Consistent with the needs of election administration as a whole, the Working Group concludes that internet ballot return has different technology needs and a different acceptable level of risk when compared to other activities we conduct on the internet.**

2. **The Working Group recommends increased investment from all levels of government for the secure and accessible administration of elections, regardless of voting method.**

3. **The Working Group concludes that the current cybersecurity environment and state of technology make it infeasible for the Working Group to draft responsible standards to support the use of internet ballot return in U.S. public elections at this time.**

4. **Internet ballot return has the potential to significantly improve upon existing solutions for accessibility and the Working Group recommends continued research and development of these technologies.**

Implementing widespread adoption of secure and accessible internet ballot return requires technologies that do not currently exist and others that have not been fully tested. There is promise, however, as technological developments have moved us closer to using internet ballot return in a secure and accessible way. Still, additional progress is necessary before standards might be developed to support the widespread use of internet ballot return in U.S. public elections, and overall cybersecurity continues to face monumental challenges.

In this statement, the Working Group addresses its belief that the underlying goal of internet ballot return is to provide an additional method for voting, particularly a method that can meet accessibility requirements specified under federal law. The Working Group provides additional considerations for research and support to that end.

The remainder of this statement lays out the rationale for the conclusions above and explores issues that could alter the risk profile of internet ballot return, making it a safe and reliable option for large-scale use in U.S. elections.

Background

Using technology to assist in the collection and aggregation of ballots has a long history; see Jones and Simons (*Broken Ballots,* 2012) for an overview.

This statement is not intended to provide an in-depth review of internet ballot return. For a comprehensive background, see the U.S. Vote Foundation's E2E Verifiable Internet Voting Project, the National Academies' The Future of Voting: Accessible, Reliable, Verifiable Technology, and the Election Assistance Commission's "A Survey of Internet Voting."

Proposals to use the internet to assist in voting are also not new (see Appel *"Is Internet Voting Trustworthy?"*, 2022, https://dx.doi.org/10.2139/ssrn.4209296). Much of this is driven by the Help America Vote Act of 2002 (HAVA) (see https://www.eac.gov/about_the_eac/help_america_vote_act.aspx).

In the United States, the Election Assistance Commission (EAC) creates and adopts the Voluntary Voting System Guidelines (VVSG) for voting systems with technical support from the National Institute of Standards and Technology (NIST).

Needed Standards for Electronic Ballot Return

The Working Group considered a basic question: what kind of standards are needed for internet ballot return and to what do they apply?

There are design standards, compliance standards, testing standards, and standards to which certifying bodies must be held, to name a few.

The applicability of those standards varies depending on implementation, and can include: the software downloaded by the user, the user device itself, servers and workstations on the administrative side, the protocols for communication, and encryption, among others.

The reality is that a lack of applicable standards in any of these could undermine the security and accessibility of any internet voting approach, and standards themselves don't ensure security.

> **While some standards may exist that would be applicable to the internet ballot return environment, the Working Group concludes that it is**

currently infeasible for the Working Group to develop the full set needed to ensure a safe and secure internet voting.

Internet Ballot Return is Not Like Other Online Transactions

A common narrative around internet ballot return goes something like this: "I bank, buy cars, and file taxes online. Why can't I vote online?"

Voting in U.S. public elections is fundamentally different from other activities performed on the internet. The reality is that several characteristics of voting – regardless of method – differentiate it from nearly all other types of activities, and thus warrant additional scrutiny before moving to an online context. Foremost amongst these characteristics are:

1. Ballot secrecy: the accuracy of typical online transactions is transparent to the participants. Customers can, for example, view their bank statements and confirm their charges. However, the standard is higher for voting. Voters should not *be able to* reveal their votes – even if they wish to do so. The ability to disclose a vote would enable vote-selling and coercion. Voters therefore cannot confirm that their votes have been correctly recorded and counted in the same way that they verify bank statements and online purchases.
2. Increased cybersecurity risks: while internet ballot return is arguably more convenient, there remain unresolved cybersecurity risks associated with it. These issues, which include malware and targeted denial-of-service (DOS) risks, are addressed in the Remaining Challenges section below.
3. Fostering acceptance of outcomes: unlike most online activities, failed – or just distrusted – elections can result in significant outcomes that affect everyone. Even the most sensitive online transactions have much lower stakes and usually impact only a few parties. Mistaken or fraudulent submissions in filing taxes and other such transactions don't result in civil unrest, for example.

The first two of these speak to technical requirements of election administration in U.S. public elections. They are artifacts of how elections get administered, and thus require different types of technology than do other types of transactions.

To underscore these points, there is a fundamental distinction between the way U.S. elections and other transactions work. In most transactions, the results of a failure are traceable and often obvious to all parties involved in a transaction: a bank account

balance is wrong, a car is delivered in an unexpected color, a tax burden does not match expectations. The intentional lack of traceability of a cast ballot back to a voter due to the requirement of a secret ballot demands different technical controls than other types of online transactions.

The third characteristic – the outsized consequences of U.S. public elections – allows for a lower level of acceptable risk than other types of transactions. This means developing technology that can both meet the technical requirements for U.S. public elections and, as importantly, do so with a lower risk of failure than is acceptable in other types of transactions and applications.

Finally, we note that an election of any sort must generate and store *credible evidence* for the reported election outcome. Voting with internet ballot return normally creates such evidence in electronic form, rather than physical form (like a paper ballot). This fundamentally changes options for providing evidence to voters that their intent has been faithfully captured.

> **The Working Group recognizes that any form of voting faces a higher burden than other online transactions in answering two challenges: what evidence is produced, and why should it be considered credible?**

Ongoing Progress

Incremental improvements in technology over the last 15 years have closed some of the gaps preventing internet ballot return from becoming a common way voters cast their ballots. These include:

- Pervasive, if incomplete, existence of high-speed internet access.
- Relatively inexpensive internet-enabled end-user devices.
- Availability of cheap, reliable authentication methods and improving, though far from perfect, digital identity proofing.
- Advances in cryptographic methods to support ballot secrecy and validation, such as end-to-end verifiability and homomorphic encryption.

On the other hand, many aspects of cybersecurity have not improved overall in the last decade: one reads weekly of breaches in major service providers that one would have hoped had the motivation and technology to do better.

The Working Group finds that such advances may seem to some to have moved us closer to secure and accessible internet ballot return, but there is still a long way to go.

> **The Working Group concludes that progress towards internet ballot return is possible, but substantial research and support**

are required to achieve a security profile that supports widespread deployment in U.S. public elections.

End-to-End Verifiability

One promising technology that is beginning to emerge has come to be known as *end-to-end verifiability (E2E-V).* This technology gives voters the ability to confirm that their votes have been correctly recorded and counted – without compromising privacy. In fact, any observer can confirm that the recorded votes have been correctly counted.

The first recommendation of the 2015 U.S. Vote Foundation study on *The Future of Voting* states that "*any public elections conducted over the Internet must be end-to-end verifiable."*

However, this technology has not yet been widely deployed in any form of public elections, and the study's second recommendation is as follows:

> *"No Internet voting system of any kind should be used for public elections before end-to-end verifiable in-person voting systems have been widely deployed and experience has been gained from their use."*
>
> - U.S. Vote Foundation study on *The Future of Voting*

While there has been progress on the deployment of E2E-V election systems and their availability has increased, there is not yet sufficient experience to make the jump to internet ballot return.

While NIST has begun some activities to evaluate E2E-V voting systems, the Working Group recommends the EAC and NIST take additional steps towards standardizing E2E-V voting systems.

Remaining Challenges

To transition internet ballot return from these less risky environments, additional research and support is needed to solve technical challenges.

The Working Group identifies numerous areas that require additional advancement for widespread trustworthy use of internet ballot return in U.S. elections. Six critical ones are:

1. **Pervasive client-side malware,**

2. **Reduced confidence through intentional malfeasance by those trying to disrupt elections,**
3. **Targeted denial of service attacks,**
4. **A lack of deployed digital credentials among potential voters,**
5. **Absence of a directly voter-verifiable ballot of record, and**
6. **Increased threat of wholesale attacks.**

The Working Group recommends that federal agencies, including the EAC, NIST, the National Science Foundation, and the Cybersecurity and Infrastructure Security Agency, put additional effort into each of these remaining challenges to advance the potential of safe and reliable deployment of internet ballot return and cybersecurity in general.

Pervasive client-side malware

The pervasiveness of malware and our inability to detect it, especially on consumer-grade devices, presents an enormous barrier to trustworthy internet ballot return schemes. While E2E-V holds promise in making malfeasance detectable, it has seen limited deployment in public elections with managed voting systems. Moving to a bring-your-own-device environment creates two issues:

1. The use of end-to-end verifiability allows voters to take steps to verify the correct recording of their votes, but it doesn't require voters to do so. When used with in-person voting on equipment provided by an election office, checks by a very small, randomly chosen fraction of voters are sufficient to provide high statistical confidence that the system is performing properly. However, when used for internet ballot return on individual devices, each voter would have to verify their own vote, ideally from a separate device that is free of malware.

   Despite the promise of E2E-V, the Working Group assesses that detecting malfeasance with widespread internet ballot return still has unresolved issues, including how voters should verify their ballots, which voters should verify their ballots, how many voters should verify their ballots, and how discrepancies (real or claimed) should be handled.

2. Consumer-grade devices with consumer-grade protections are no match for a motivated attacker, particularly if the attacker is a nation-state. Most transactions conducted on such devices don't rise to the level of nation-state interest, but voting does.

The Working Group assesses that the risks associated with nation-states attacking end-user devices to impact U.S. public elections are problematically high and show no signs of declining.

In addition, the Working Group notes that having to deal with malware on consumer devices is a problem that doesn't exist for other modes of voting.

Reduced Confidence Through Intentional Malfeasance

A related risk is the ability of an individual or small number of individuals to undermine confidence in an election by fraudulently claiming failed verifications or intentionally introducing malware into their or other individuals' devices. Confidence in U.S. election administration is already troublingly low, even though there is no evidence of fraudulent activity at any significant scale.

The use of consumer-controlled devices and a lack of a paper trail creates a high likelihood that a malicious actor will intentionally use malware or falsify evidence of fraud to further erode confidence in elections.

Additional research is needed to reduce a user's ability to intentionally generate fraudulent results when consumer devices are used in U.S. public elections. To mitigate this risk requires an improved ability to debunk fake results.

Targeted denial of service attacks

Denial of service attacks present a nuisance, sometimes a costly one, for most online transactions. In the context of elections, however, an attacker could change the outcome by simply impeding service in a targeted region or demographic. Extending deadlines or retransmitting activity are an easy fix for most service disruptions, but they are a political, logistic, and, potentially, constitutional concern in U.S. public elections.

While reasonable mitigations for denial-of-service attacks are effective in most contexts, the consequences associated with U.S. public elections are high enough that the Working Group sees targeted denial-of-service attacks as a major risk to elections that leverage large-scale internet ballot return.

Additional efforts are needed to improve resilience to denial-of-service attacks. Specifically, work is needed to understand how third-parties can regulate the flow of

cast ballots mixed with other content on the internet while maintaining accountability. Such third parties should not be able to bias the outcome by letting only certain ballots pass through.

A Lack of Deployed Digital Credentials

Voter identification is a contentious issue, but in internet ballot return, strong verification of identity is an indispensable part of the process. At internet scale, it would be effectively impossible to stop widespread fraud without strong digital credentials. In today's environment, strong authenticators and quality remote identity proofing are possible, but the latter can be costly and has high failure rates for underserved populations. Indeed, the complications for verifying voter identities over the internet could undercut any convenience and accessibility justifications for internet ballot return. Emerging technologies like mobile driver's licenses hold promise, but are not yet in wide use and do not fully address the needs of underserved populations. Furthermore, such digital credentials would need to be coordinated with voter registration.

> **The Working Group finds that the lack of available digital credentials strongly tied to an individual is a significant barrier to widespread use of internet ballot return, a problem that will likely require substantial engagement, and likely federal action, to establish a meaningful floor for security without undercutting inclusion.**

Absence of a directly voter-verifiable ballot of record

Internet ballot return has a ballot-of-record that is electronic, rather than physical. Voters can not directly verify that an electronically cast ballot faithfully represents their selections. Voters must therefore use some electronic system (e.g., their smartphone) to verify that their selections have been accurately recorded and cast.

Since such an electronic system is itself corruptible, verification must work in spite of corrupted software. Otherwise the electronic system could cheat the voter by claiming to have cast the vote one way, and actually casting the vote a different way. Usability is important here, as is the development of guidelines for handling disputes, when voters find (or claim) that their voters were not accurately recorded or cast.

> **The Working Group determines that further research is needed to develop protocols that can be used by voters to cast their votes using personal devices and verify that their votes have been accurately recorded and cast.**

Increased Threat of Wholesale Attacks

With in-person voting and vote-by-mail, the damage that can be inflicted by a small number of individuals is limited. Although no method of voting is completely immune to attacks and corruption, it is very difficult for a small group of attackers to impact a large number of votes.

However, when internet ballot return is employed, it may be possible for a single attacker to alter thousands or even millions of votes. And this lone individual could perpetrate an attack from a different continent from the one where the election is being held – perhaps even while under the protection of a rogue nation where there is no concern of repercussions.

> **The Working Group recognizes that current approaches to internet ballot return carry larger risks of wholesale attacks than other common voting methods, and that these risks create more significant consequences for election outcomes.**

Balancing Security and Accessibility

Finally, while the Working Group believes it is currently infeasible to draft responsible standards on internet ballot return, it also recognizes that all current methods of voting have risks that must be carefully managed and all present benefits intended to serve the varied needs of voters.

Some forms of internet ballot return, including email, fax, and file transfer protocol server, present a risk to the security of elections, even relative to internet ballot return methods commonly called mobile voting. At the same time, they can be an important tool for accessibility and ballot access for overseas voters; voters for whom getting to the polls may be difficult; individuals who, due to physical limitations, may have difficulty accessing a traditional polling site; and others who struggle to, or simply cannot, use traditional voting methods.

Eliminating these forms of voting entirely without reasonable alternatives could produce an unacceptable risk to those with accessibility needs and would place election officials in a position of violating the requirements of the HAVA and the Americans with Disabilities Act (ADA), expanding them could present unacceptable security risks to those same voters and the integrity of the election.

> **The Working Group recognizes that those administering elections are the final arbiters of risk and must consider voter needs and federal and state legal requirements regarding accessibility, in addition to security risks, when making decisions about voting methods.**