U.S. Election Expert Perspectives on End-to-end Verifiable Voting Systems

Julie M. Haney*, Shanée Dawkins*, Sandra Spickard Prettyman†, Mary F. Theofanos*, Kristen K. Greene*, Kristin L. Kelly Koskey†, and Jody L. Jacobs*
*National Institute of Standards and Technology, Gaithersburg, Maryland 20899
Email: human-cybersec@nist.gov
†Cultural Catalyst LLC, Chicago, IL 60605

***Abstract*—By using cryptographic techniques, end-to-end verifiable (E2EV) voting systems have been proposed as a way to increase voter trust and confidence in elections by providing the public with direct evidence of the integrity of election systems and outcomes. However, it is unclear as to whether the path to E2EV adoption for in-person elections in the United States is feasible given the confluence of factors impacting voter trust and technology adoption. Our research addresses this gap with a first-of-its-kind interview study with 33 election experts in four areas: accessibility, cybersecurity, usability, and general elections. We found that participants' understanding of and opinions on E2EV diverged. While E2EV was lauded by some for increased security and transparency, others described it does not address major challenges to voter trust in U.S. elections and might actually have a negative impact due to complexity and limitations. Overall, participants recognized that the feasibility of widescale E2EV adoption hinges on not just the strength and security of the technology, but also on consideration of the people and process issues surrounding it. Based on our results, we offer suggestions for future work towards informing decisions about whether to adopt E2EV systems more widely.**

I. Introduction

The United States (U.S.) Help America Vote Act of 2002 (HAVA) created a U.S. federal government infrastructure to help realize nationwide improvements in voting systems [1]. A key component of HAVA was the creation of the Voluntary Voting System Guidelines (VVSG), a set of specifications for ensuring voting systems meet standards for basic functionality, accessibility, and security [2]. In addition to improving voting system technology, these guidelines have an added benefit of working to bolster voter trust and confidence in elections, which, as researchers observed, have declined in recent years [3].

To mitigate cybersecurity risks and build public trust in voting systems and processes, the latest version of the guidelines, VVSG 2.0 adopted in 2021, requires that voting systems be auditable [4]. The guidelines identify possible methods to meet the auditing requirements, including paper-based records, ballot images, risk-limiting audits, and *end-to-end verifiable voting (E2EV) systems* for in-person voting, the focus of this paper. Through the use of cryptography, E2EV allows voters to check that their votes are both cast as they intended and included in the final vote tally. In addition, the public can verify that all recorded votes are included in the tally [5].

E2EV was included in VVSG 2.0 even though a formal process to evaluate E2EV protocols and products has not been developed. During the initial work to define a process, election officials (those responsible for administering elections) and others working in the elections space expressed that the influence of non-security factors—such as usability, accessibility, and voter perceptions—on E2EV adoption should be considered before substantial effort is spent developing detailed technical specifications and certifications [6]. These views illuminate the currently unmet need for a holistic exploration of the potential opportunities, benefits, and challenges of E2EV that take into account the interactive web of people, processes, and technologies related to voter trust and confidence [7].

We conducted exploratory, qualitative interviews to fill this gap, with study bounds set by our funding institution, a U.S. governmental agency that helps election officials improve U.S. election administration, voter participation, and election safety and security. The scope was *considerations for E2EV adoption for in-person voting in the U.S.* towards informing decisions about future E2EV standards and investment. Specifically, we interviewed experts with influence in U.S. elections and deep knowledge in subject areas relevant to E2EV, voter trust, and voting technologies, as explicitly highlighted in the VVSG. These areas included: accessibility, cybersecurity, usability, and general election expertise (administration and provision of support to elections, for example, former election officials or members of election standards or consulting organizations). In total, we interviewed 33 experts in 32 interviews.

Since we had interest in exploring how E2EV is situated within the larger elections ecosystem, in addition to a line of inquiry about E2EV, the interview protocol covered broader topics related to current and future technological and non-technological challenges to voter trust and confidence. While we summarize participants' views on these broader challenges in Results, we do so to provide context for our E2EV findings. This paper more pointedly focuses on a subset of our findings towards answering the following research questions:

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23035
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

RQ1: What are election experts' perceptions and understanding of E2EV and its adoption feasibility?

RQ2: In what ways, if any, do election experts believe E2EV might impact voter trust and confidence in elections?

Our study makes several contributions. We extend the broader base of election research knowledge by conducting a study that holistically and descriptively identifies potential benefits and challenges of E2EV from the *perspectives of election experts from diverse disciplines*. While other research teams previously conducted research on verifiable voting, our scope is unique to these works in several ways. First, rather than voter-focused research (e.g., [8], [9], [10], [11], [12],), we explored the space through the eyes of election experts in roles that directly impact voting technology adoption decisions. Second, much prior E2EV adoption research in the U.S. was conducted years ago (e.g., [13], [14]), so it does not reflect the current U.S. election landscape that we explore. Third, instead of the online (internet) voting focus of most prior work–which introduces its own complexities, biases, and voter misconceptions [15], [10], [16], [12]–we address E2EV for *in-person* voting. Finally, our study was specific to the U.S., which has different election sensitivities and processes [17], [18] than the European countries represented in much of this body of literature (e.g., [8], [19]).

Overall, this exploration provides novel insights related to 1) the feasibility of widespread adoption of E2EV voting systems in the U.S., 2) whether E2EV has the potential to increase voter trust and confidence in U.S. elections, 3) E2EV uncertainties and issues warranting further exploration and solutions, and, consequently, 3) if the substantial work needed to engage the U.S. election and cybersecurity communities in developing an E2EV evaluation process would be prudent.

II. Background and Related Work

We summarize factors influencing voter trust and confidence in elections as a foundation for exploring E2EV's potential role. We then provide background information on E2EV, including an overview of the technology, prior research, real-world E2EV applications, and the significance of E2EV's inclusion in U.S. election system guidelines.

A. Voter Trust and Confidence

Voter trust and confidence in U.S. elections are influenced by myriad factors. Personal experiences throughout the voter journey–including interactions with election workers, changes to voting technologies and processes, and the usability and accessibility of technologies and processes—play a major role [20], [21], [22], [7]. Additionally, voters' (lack of) understanding about the complexity of U.S. elections can impact trust and confidence [23]. For example, in the U.S., elections are administered locally, with states and local jurisdictions often having their own election laws, requirements, technologies, and processes. Although voters tend to trust their local elections, they may distrust and misunderstand the processes of other jurisdictions that do things differently [24]. Our study explores how E2EV might be situated within this complex aggregation of factors influencing voter trust and confidence.

B. End-to-End Verifiable Voting Systems

1) Technology Overview: Researchers first proposed the concept of end-to-end verifiability in the 1980s as a way to use cryptographic algorithms to provide for both anonymous voting ballot submission and the verification of tally accuracy by external observers [25], [26]. While this research area has evolved over the years, E2EV is generally described as consisting of three key aspects [5]:

1) **Cast As Intended:** "Voters make their selections and, at the time of vote casting, can get convincing evidence that their encrypted votes accurately reflect their choices."
2) **Recorded As Cast:** After voting, voters are able to verify that their vote has been recorded. A common method of verification involves a code (e.g., a URL or QR code). The code allows voters or their designees to "check online that their encrypted votes have been correctly included, by finding exactly the encrypted value they cast on a public list of encrypted cast votes."
3) **Tallied As Recorded:** Any member of the public (typically at the institution level) can write a verifier to "check that all published encrypted votes are correctly included in the tally, without knowing how any individual voted."

Post-election audits to verify that votes are accurately recorded and counted–such as hand counting or risk-limiting audits (RLAs)–are not new to elections. However, E2EV claims to have the added benefit of public involvement, while still protecting voter privacy.

2) Online Verifiable Voting Research: A body of literature about E2EV (called verifiable voting in these works) documents voter-focused research conducted for online (internet) voting applications. Helios, an early E2EV system for online voting, was deployed as a trial in a Belgian university election [27], [28]. However, subsequent research evaluations uncovered a number of usability issues, with representative voters finding the verifiability process to be complex, time intensive, and error-prone [13], [29].

Subsequently, European studies identified factors influencing voter trust of newer online verifiable voting systems. Usability, trust in the authorities controlling the system, prior technology trials, ability to self-verify, and voter support services (e.g., helpdesk) positively impacted voter trust in Germany and Switzerland [19], [10]. In Estonia, institutional trust was key to confidence in the online voting system [30]. Conversely, perceptions of low security, uncertainty on how verification failures are handled, perception that privacy is not maintained, and burdensome interfaces had negative impacts [19], [9], [10]. A Swiss group discovered differing levels of sophistication, security concerns, understanding, and expectations in voters' mental models [12]. They found that misconceptions of how voting systems work did not necessarily impact willingness to use the systems. However, another team found that voters need some understanding of why they should verify their vote or else they will not do so [19]. Regarding

perceived usability-security tensions, one found that voters, if educated properly, would be willing to sacrifice usability for security in internet voting [31]. Another suggested that, while perceptions of low system security could discourage voters from adopting a technology, an inflated perception could lead to voters engaging in insecure practices [19].

While voter perspectives–the focus of these explorations–are important for technology acceptance, our study explores E2EV through the lens of experts with influence on adoption decisions. Additionally, while most of these prior works focused on usability and security, we also address the interactions of those with accessibility and election administration. Finally, in contrast to European online voting contexts, our research is specific to *in-person* U.S. elections.

3) Real-World Applications: There have been several implementations of E2EV for in-person elections. Early solutions included Prêt à Voter [32] and Scantegrity II [14]. However, these were met with criticism from usability researchers who, in laboratory experiments, found that the systems resulted in difficulties casting votes, low ratings of satisfaction, confusion about the purpose of the technology, and low likelihood of vote verification [13], [8], [9]. A more recent instantiation of E2EV is ElectionGuard, an open source E2EV software development kit that uses homomorphic encryption [33].

To date, E2EV has been used in four small U.S. elections: a municipal (local) election in Takoma Park, Maryland in 2009 using Scantegrity II [14]; a municipal election in Fulton, Wisconsin in 2020 using ElectionGuard [34]; a national election in Preston, Idaho in 2022 using ElectionGuard [35]; and a municipal election in College Park, Maryland in 2023 using ElectionGuard [36]. Ensuring good voter communication and outreach–via town hall meetings, opportunities for practice voting, plain-language pocket guides, and consistent explanations from election workers–was viewed as critical in all four instances. Exit interviews revealed voter thoughts about the E2EV implementations. In contrast to prior E2EV laboratory experiments (above), voters responded positively to the implementations, reporting few difficulties and appreciating the capability to review their votes and later confirm their votes had been counted [14], [37], [38], [39]. Many said that the new capabilities improved their confidence in the election process and that they were encouraged to see local election officials "keeping up with the times" [39]. However, as in the laboratory studies, some voters expressed concerns, including confusion about the process and what the technology was doing, whether there was a need for the added security since they already trusted local elections, and uncertainty if some groups of voters (e.g., older voters) would be able to understand or use the confirmation codes to verify votes [14], [38], [39].

While these real-world implementations illustrate the potential benefits of E2EV for voters, they show that usability issues remain. Additionally, as there have only been a few examples of E2EV use in U.S. elections, it is uncertain if voters in other U.S. localities would respond similarly or if election officials en masse would be open to E2EV. We also note that the exit interviews were limited in that they did not explore voters' experiences when checking their ballots after they left the polling location. Our study extends findings from these specific implementations by providing a wider view across the election community and identifying potential barriers that must be overcome for large-scale E2EV adoption.

4) U.S. Voluntary Voting System Guidelines: As E2EV has matured, it has gained increased interest from the U.S. Government and other voting groups as a potential way to increase both election security and voter trust and confidence in elections [40], [41]. VVSG 2.0–adopted by the U.S. Election Assistance Commission (EAC) in 2021–includes E2EV as a possibility for a requirement to ensure "the voting system is auditable and enables evidence-based elections" [4]. Part of this requirement involves the use of software independent systems. Software independence is the "Quality of a voting system or voting device where a previously undetected change or fault in software cannot cause an undetectable change or error in election outcome" [42]. VVSG 2.0 includes two paths for software independence: 1) paper-based system architectures and 2) E2EV system architectures. Further, the guidelines state that any E2EV systems must use approved cryptographic protocols and undergo an independent evaluation of its implementation of an approved protocol [43].

However, there are currently no technical specifications or evaluation procedures for E2EV. To begin discussing these specifications, in 2022, the EAC, National Institute of Standards and Technology (NIST), and National Cybersecurity Center of Excellence (NCCoE) conducted a workshop, *The Path to End-to-End (E2E) Protocols for Voting Systems* [6]. NIST voting experts acknowledged that development of E2EV specifications would likely require substantial effort due to a number of challenges, including: current use of non-standard cryptographic algorithms in E2EV solutions; need for subject matter experts to review the cryptographic protocols; E2EV's unique usability and accessibility challenges due to its reliance on voter verification; and the need to ensure that E2EV systems are implemented to be software independent and secure to avoid errors and preserve ballot secrecy.

Moreover, election expert panelists representing the election administration, usability, accessibility, and cybersecurity communities stressed that more thought should be given for non-technical people and process factors that would contribute to the long-term feasibility of E2EV. For example, several panelists expressed hesitation to make large-scale technology changes to elections, which could potentially add more burden to election workers or raise questions among voters. Through a rigorous, systematic research process, our study begins to provide this additional, holistic evidence to inform decisions about investment in efforts to develop E2EV specifications.

III. Methodology

To explore election experts' perceptions and views on the potential of E2EV to impact voter trust and confidence in elections, we took an exploratory, qualitative research approach.

A. Study Design

1) Informing the Study Design: Prior to study design, we conducted fieldwork to observe E2EV in a real-world election to give us greater insight into the topic at hand. First, several team members attended a pre-election meeting that presented voters with an overview of the E2EV technology and an opportunity to try out the voting systems. Subsequently, we observed inside a voting place on election day to see firsthand the use of the technology, interactions of poll workers and voters, and flow of the voting process. After the observations, we recorded field notes and met to debrief and discuss.

Based on this field research and a review of related works, we developed research questions and decided upon a multiple case, qualitative interview approach. A multi-case study was appropriate for our research because it allowed for inclusion of a range of experts involved in different aspects of voting processes, providing insight both within and across those groups to understand the phenomenon [44], [45]. Further, this method strengthened study reliability by confirming expert opinions where consistent patterns emerged across groups [44], [45]. Defining and bounding the case(s) of interest is also important [45]. In the current study, a case was bounded and defined at three levels: individual election expert participants (level 1) were nested within one of four election expert groups (level 2) and the entire group of election experts (level 3). Overall, *qualitative description* was a major goal of the case study towards better understanding the phenomenon in participants' own words [46], [47].

2) Sampling Strategy: A small number of cases (4-10) that represent the diversity of the context is recommended for multiple case studies [48]. As such, we sought the perspectives of election experts from four areas (cases): accessibility, cybersecurity, usability, and general election expertise, a proxy for election officials that included individuals with substantial experience in administering and supporting elections. We chose these four areas of expertise for their foundational importance in elections and voting technologies, emphasis in the VVSG, and the known tensions or "tradeoffs" between them (e.g., security vs. usability) [20], [6], [22], [7]. Additionally, these groups represent those who would ultimately decide to adopt E2EV (i.e., state and local election officials), as well as other election experts who might advocate for or against E2EV to both voters and election officials, influence or develop E2EV solutions, or understand how E2EV fits within the larger U.S. elections ecosystem. Our intent in sampling across groups was to capture a broader, representative range of perspectives to support a more holistic description, rather than limiting our analysis to a narrow view of individual expert groups.

We ensured that we recruited a number of participants with expertise in E2EV, both from theoretical and practical perspectives, including experience with real-world election implementations. However, a majority were not E2EV experts. Had we only sampled E2EV experts, results would be biased and missing other important voices with influence over voting technology standards and adoption. It was important to identify whether well-respected election community leaders had awareness and understanding of E2EV, and whether they believed E2EV addressed major challenges impacting voter trust. If not, widespread adoption would be unlikely.

3) Interview Protocol Development: We developed semi-structured interview protocols for each expert group in alignment with the research questions. Protocols were reviewed by four subject matter experts (one from each expert group) and an expert in qualitative research (25+ years experience). Reviewers suggested that the focus on E2EV and technology was too narrow to address E2EV's place within the larger election ecosystem. Thus, we made revisions to the protocol to expand the focus towards addressing how E2EV might be situated within the most salient current and future challenges to voter trust and confidence in elections. Additionally, reviewers provided comments related to language and question ordering that resulted in changes to the interview instrument. The revised protocols then went through another round of reviews with the same subject matter experts, followed by four pilot interviews (one of each group), with minor changes made to address wording and flow. Because modifications were minor, we included the pilots in our final data set.

We first asked participants to describe their background and current role with respect to elections. Across expert groups, we then asked a set of six common lines of inquiry: (a) the biggest technological and non-technological challenges to voter trust and confidence in elections today, if any, (b) challenges that may still be around in the future, well beyond the 2024 election, (c) how voter trust and confidence in elections can be improved, if at all, (d) the future of election technology, (e) experts' own level of trust and confidence in elections, and (f) understanding of E2EV, and, if familiar with the concept, how these might impact voter trust and confidence in elections. We also used tailored follow-up questions for each group related to their respective areas of expertise. For example, cybersecurity experts were explicitly asked to describe cybersecurity challenges. See Appendix A for an example protocol.

B. Data Collection

To identify information rich cases, we used purposeful sampling to recruit via email from each expert group. We initially collected names of potential participants from our team's previous voting connections. Additional snowball sampling allowed us to reach data saturation for each group, focusing not just on number of interviews, but depth of data [49].

We conducted virtual interviews March to June 2024. Interviews lasted 39 to 62 minutes (M = 47.5 minutes) and were recorded and professionally transcribed. A total of 33 election experts participated in 32 interviews across the four groups: accessibility (n = 8), cybersecurity (n = 9), general elections (n = 9), and usability (n = 7).

C. Participant Backgrounds

Given the relatively small community of election experts in the four areas of interest and the threat environment that

members of the U.S. election community face [50], we protect participants' confidentiality by reporting participants' expertise in aggregate rather than per individual.

Participants came from various sectors, including industry, government, non-profits, and academia. All were actively involved in or had recently retired (within a year) from the election space at the time of the interviews. Of the 28 participants who reported years of election experience, experience ranged from 10-40+ years with a mean of 23.5 years. Together, these experts had over 630 years of election experience.

Participants were well-respected leaders in the election space, having experience in a variety of high-impact positions, for example: executives of national organizations; voting equipment procurement experts; election consultants; well-published researchers and authors; voting technology vendors; expert legal testifiers; election budget and policy makers; voter education and outreach developers; and members of voting standards and working groups. Ten participants–including 8/9 general election experts–formerly served in election administration roles, with all others having experience supporting election officials. Further, many were intimately familiar with voter needs and challenges, having experience conducting voter research or working with and on behalf of voters.

Accessibility experts included researchers, leaders of advocacy networks for voters with disabilities, and contributors to accessibility standards and policies. Cybersecurity experts included cryptographers, researchers, product developers, and those working in election security and integrity. Usability experts had research and practitioner backgrounds in human factors in voting, including human-centered design of voting ballots, education materials, and systems. General election experts had prior election administration experience at local and state levels or served as consultants to election officials.

D. Data Analysis

We conducted data analysis following Braun and Clarke's thematic analysis process [51], [52]. We initially created a short list of *a priori* codes based on the literature, the research questions, and our team's previous experience in the voting space. To become familiar with the data, we read the interview transcripts and memoed initial thoughts. We then generated ideas for additional, emergent codes based on team review and discussion of two interviews, one from a cybersecurity expert and another from an accessibility expert. Subsequently, four researchers independently coded four interviews, one from each of the election expert groups to develop the initial code list. Using this initial codebook, six researchers then independently coded the four interviews and then engaged in whole-team coding discussions to refine and clarify the coding scheme. We further operationalized (formally defined) each code to facilitate consistent use by all coders. The final codebook used for this paper (Appendix B) included 12 overarching parent codes, with some consisting of subcodes reflecting the dimensions of participants' descriptions falling within the parent code. For instance, three subcodes were nested under the parent code *Voters* to distinguish among expert participants' descriptions related to voters' expectations, influences on voters' trust and confidence in elections, and voters' knowledge and understanding of elections.

We then applied the codebook to all 32 interview transcripts in coder pairs. Within coder pairs, researchers independently coded a transcript and then met to compare and settle on final codes, focusing not just on agreement but also on how and why disagreements in coding arose and the insights afforded by subsequent discussions [53], [54]. Each coder pair also generated memos outlining a synopsis of each interview and subcategories of higher-level codes (e.g., Resources under Challenges). These memos focused on identifying major takeaways from the interviews, including perceptions of the impact of E2EV voting systems on voter trust and confidence.

In ongoing whole team meetings, we worked to identify major themes emerging from the data. We then diagrammed these ideas to further analyze how they connected to larger concepts in the data, such as voter trust and confidence. These diagrams helped us to explore if and how these overarching themes helped answer the research questions and the role they played in addressing the problem under study.

E. Positionality

Our multidisciplinary team of researchers brought a variety of perspectives and experiences to the work. The team has expertise in computer science, human factors, cybersecurity, psychology, sociology, and qualitative research methods. Two team members also had prior experience conducting voting usability and accessibility research. The variety of backgrounds contributed a richness and depth to the project, but also moved us beyond our own intellectual comfort zones. This was particularly valuable when analyzing data in a multiple case study. The multidisciplinary nature of the team also strengthened the research quality "in terms of enabling sounder methodological design, increasing rigor, and encouraging richer conceptual analysis and interpretation" [55]. Additionally, most of the team were U.S. Government employees. Our research was funded by an external government agency with authority in the development of technical guidelines in the voting space. Our role was not to definitively determine whether E2EV is a viable solution at scale, but rather to provide descriptive evidence to decision makers.

F. Ethics

The study was approved by our human subjects institutional review board. Participants provided verbal consent, and all questions were voluntary. We protected confidentiality by redacting identifiable information from research records and assigning anonymous identifiers (e.g., G8). See Appendix C for more details on our ethical considerations.

G. Limitations

Our study has several limitations. 1) While we purposely selected four expert groups to provide a holistic perspective, we did not perform in-depth comparisons between groups. Future research could extend our work to glean differences

and tensions between groups. 2) Because we had an in-person, U.S. voting scope, our findings may not be generalizable to other countries or online voting. 3) Given the time constraints of election officials in a presidential election year (2024) and the short timeline enacted by our funding institution, we did not speak directly with current election officials. Although the experts in our study all had extensive experience in the election space, future interviews with current election officials could provide additional insight on the potential of E2EV. 4) As these interviews were conducted prior to the 2024 election, we recognize that the experience of that election may have changed the voting landscape in ways that we could not know in advance. Another round of interviews post election, even with the same election experts, might uncover different topics, ideas, or perspectives, which could further augment the findings from this study. 5) While many participants were quite familiar with voter needs and behaviors, our study does not reflect the direct views of voters.

IV. Results

We summarize participants' views on challenges to voter trust and confidence in elections today, followed by in-depth examination of the opportunities and challenges of E2EV identified by—-and in the direct words of—-participants. Of particular note, most participants discussed E2EV only when prompted during the last set of E2EV-specific questions. However, 11 participants (including six cybersecurity experts) organically mentioned the technology earlier in the interview. Throughout, we provide exemplar quotes with participant reference codes to illustrate themes. The letter at the beginning of each reference code indicates the expert group: A = Accessibility; C = Cybersecurity; G = General Election; U = Usability. This is followed by the interview number (e.g., G8).

A. Challenges to Voter Trust and Confidence

> "My thought is that the biggest challenges right now...are not with the technology, but are with the people side of things"
>
> *Participant C2*

Participants voiced major challenges to voter trust and confidence in U.S. elections. Two cross-cutting concepts-–inherent complexity of U.S. elections and the omnipresent, dynamic information environment—permeated the challenges. These concepts were the most mentioned when participants were first asked about the "biggest" challenges and then later asked for the top three "most pressing" challenges.

Limited or incorrect voter knowledge and understanding about election methods, processes, and technologies, according to participants, is due in large part to the complex, dispersed, and intermittent nature of U.S. elections. Participants described a disconnect between voters' understanding of elections and reality: "most people think elections are very simple and that they have a good understanding of how they actually work when, in fact, elections are very complicated" (U5). Participants also said that the dynamic information environment can present conflicting or confusing content.

Unrealistic or unmet voter expectations during the voter journey were another significant challenge expressed by participants. According to the experts, disconnects between expectations and personal experiences–such as negative experiences while voting or changes in election processes or technologies–can challenge mental models about elections and erode trust: "people become comfortable with one technology, and that technology stops being used. So now they have to sort of reacquaint themselves and officials have to find new ways of reassuring voters about how these systems work" (C4).

Inefficient allocation of election resources was noted by participants, who felt that episodic funding schedules could be challenging for election officials to manage. According to participants, difficulties accessing and managing resources can hamper election officials' efforts to maintain or increase voter trust and confidence in elections, for example, by impacting their ability to upgrade voting systems or limiting "the amount of communicating they could do with voters" (G5).

The need for usable, accessible, and secure technology was seen by participants as an important and challenging requirement in the election landscape. For example, one participant said that it is incumbent to design systems "that people can understand and feel confident in" (C2). Participants also expressed that there is often a tension between security and the need for more usable and accessible technology and that these shortfalls might cause voters to disengage and distrust. Yet, participants expressed that technological challenges are not as pressing as the other challenges.

B. Describing E2EV Voting Systems

> "You are able to cast your vote and then afterwards check to ensure that it was counted accurately... Now, I have all kinds of questions about how that would work in practice"
>
> *Participant U2*

We ensured participants understood what E2EV was before asking about E2EV benefits and challenges by requesting that participants briefly describe what an E2EV voting system is, in their own words. Thirty participants attempted to describe E2EV. The three who did not (two accessibility and a general elections expert) had heard of it, but admitted they knew little. To determine participant understanding, a research team member with voting expertise qualitatively assessed the participant explanations to determine if any of the three elements of E2EV (II-B1) were included or if inaccuracies were present. A second researcher then reviewed the assessments.

Twenty-two (including all cybersecurity experts) provided a reasonable (inclusion of at least one E2EV element), but sometimes incomplete, description of E2EV, with another demonstrating expertise in their comments but not providing a succinct description. U1 described *tallied as recorded*: "allowing independent verification of the mathematical accuracy of the election results." C4 referred to all three elements:

> "An [E2EV] system is one in which it's possible for a voter to confirm not only that their ballot was counted, but that it was counted correctly and included in the

tally as well as possible to verify that all of the other cast ballots were tallied correctly."

Beyond the three elements, several experts described E2EV systems as providing an evidence trail. A participant reflected that E2EV systems allow voters to follow their ballot "throughout that system and know that the vote was counted in the way that they cast it" (C7). C1 said that E2EV provides "a public, encrypted snapshot of an election for everybody to scrutinize."

In addition to the 22, five (three accessibility and two general election experts) provided a partially correct description with some inaccuracies. Four had a misconception about preservation of ballot secrecy: "it's based on an individual to be able to know and verify who they voted for and track that all the way...to make sure that their actual intended selectees were the ones that were counted for them" (A7). Two mistakenly thought E2EV is synonymous with ballot tracking: "It means that the vote ballot can be tracked without the vote being tracked" (A6).

C. Assessing E2EV Potential Impacts

"You can't create voter confidence with math."

Participant C7

We present participants' thoughts on the benefits and drawbacks of E2EV regarding voter trust and confidence. The divide in opinion was not always consistent across expert groups. For example, since E2EV claims increased security, one might think that most of the cybersecurity experts would be positive about the technology. However, this was not the case, with six cybersecurity experts voicing doubts about the potential efficacy and practicality of E2EV. Of particular note, usability experts were largely negative, with other groups split.

1) Potential to Support Evidence-Based Elections: **Some participants thought E2EV has the potential to engender voter confidence by providing evidence that election outcomes are correct.** Several participants advocated for "evidence-based elections" (C3), with E2EV being one method to achieve these. A cybersecurity participant expressed, "Instead of telling voters that they should trust the results, 'There are good people doing it, don't worry,' we should be giving voters direct evidence so that they can see for themselves that their votes are being accurately counted" (C3). A usability expert said that E2EV allows for a definitive "mathematical audit" (U1) to verify vote tallies. Another likened E2EV to a "kind of zero trust for elections" (C1). C6 expanded on this:

> "We're trusting that election administrators run the audit properly. We are trusting that the tabulators have been properly maintained...There's all this delegated trust. And end-to-end verifiable..., there's no such thing. The math can help you figure it out."

Participants expressed that public involvement to check the evidence is a key benefit of E2EV over other types of compliance-based or risk-limiting audits:

> "that I know that I, as a layperson, can test it and then really super smart outside computer folks can test it, I do think those two things go a long ways towards creating one extra level really of trust in the veracity of the system and the integrity of the outcome" (U7).

Other experts mentioned that the potential of having multiple third-party organizations—such as academic, news, political, or non-partisan organizations—write independent verifiers to check election results could provide even more confidence. Voters could then consult whichever verifier they most trust: "you would have these trusted sources of information come out and say that we have a safe and secure system" (A2).

Others voiced concerns that getting voters to take the extra verification steps may be difficult. In E2EV, while voters ensure their votes are cast as intended during the act of voting, participants noted that the later verification step to ensure their votes are recorded as cast is "entirely optional" (C3). A number of participants expressed concern about whether enough voters would take the extra verification steps:

> "The mental model that most people have of how to vote is: you make your selections and submit them, and that's the end of the game, right? So E2E systems, in order for them to actually do what they want to be doing, require at least some number of the voters to perform extra actions, right, to do verifications and to do whatever. And I think it's always a challenge to motivate voters to perform those extra steps" (U5).

Experts believed that the verification process may influence whether voters take the extra steps. For example, some E2EV systems provide voters with a paper receipt containing a confirmation code (e.g., alphanumeric or QR code) for verification, but it was unclear to the experts if this method is easy for all voters. If the process is not usable, voters "may do it once and say, 'Oh, that was hard. It's not worth the trouble,' and they may not do it again" (A8).

Several participants noted that E2EV systems are limited in what they can do. Experts with deeper E2EV knowledge emphasized that these voting systems are, in effect, an after-the-fact auditing mechanism and are not proactive or prescriptive: "the verifiable technologies that we have are all about detection of anomalies. They're not about prevention." (C3). These participants further noted that, while an E2EV system can identify an issue with the final tally, it cannot provide details on why the anomaly happened or how to remedy it, i.e., "dispute resolution" (C3). Several discussed how this limitation could negatively impact voter trust and confidence in the election process. One expert noted potential issues if a verifier–either correctly or incorrectly–identified an error:

> "If you discover that something went wrong,... what you get is that, oh, the system doesn't actually verify the correct count. And so it's got a large potential for a relatively small error to appear that the election has been completely compromised. And that actually has the potential to make things worse rather than better. That could unnecessarily decrease confidence in what may be moderately flawed but still fundamentally sound election procedures" (C4).

A usability expert imagined how E2EV might be susceptible to mistaken claims of voting system failure if:

> "large numbers of people report that their vote wasn't accurately recorded... And I really haven't spent enough time talking to people who are working on these systems for how you get around that problem, or people misremembering how they vote and saying that it was inaccurately recorded" (U2).

Several suggested that discrepancies be addressed by using paper ballot records as a fallback, which some E2EV systems already do. Additionally, another participant emphasized that transparency is an important part of voter trust of confidence: "it's a fair criticism... 'I don't want voters to know that something is wrong if they have no way of showing anybody else. That's just going to create greater chaos.' I will claim otherwise. I will claim that knowledge is power" (C3).

2) Complexity: **Participants were concerned that E2EV would introduce another layer of complexity that may be difficult for voters to understand.** One of the most-frequently mentioned downsides of E2EV in the interviews was that E2EV systems are complex, adding to an already complicated election ecosystem. Even participants who were positive about E2EV acknowledged that the underpinnings of this technology include "a lot of mathematics that most people are not going to understand" (C3).

Some experts feared that, because E2EV is so complex, its use might result in misunderstandings that could dampen voter trust and confidence. Several participants noted that a challenge to E2EV adoption was "adjusting people's mental models to be able for them to sort of understand what that even means and why they need it" (U5). One participant worried that the individual voter verification process could be wrongly interpreted as being a way to confirm online how someone voted: "[E2EV systems] are generally very clever to prevent that receipt from actually revealing to a third party how someone voted, [but] they could create the impression among voters that their vote isn't secret anymore" (C4). Conversely, during the post-voting verification process, participants predicted that some voters may want to see if their votes were cast as intended (rather than just recorded as cast), resulting in a mismatch between their expectations and reality since verification does not reveal a voter's selections:

> "all of a sudden, I'm getting a string of codes. It's like, 'This isn't what I wanted. What I wanted was to see my ballot in the ballot box.' 'Well, no, we can't do that because of X, Y, and Z ballot secrecy...what we're doing is letting you know it's been unchanged' " (G4).

Multiple participants expressed that voters today are demanding more transparency in elections. However, they felt that E2EV systems may appear to be a mysterious "black box" (U3). As one participant said: "saying to voters, 'Just trust the math,' is not acceptable" (G5). Further, several participants expressed concern about the introduction of E2EV as a deeply technical solution when some voters may not trust technology. This "checking technology with technology" (G3) scenario could increase distrust. Another echoed this concern: "no matter how we build in an end-to-end verifiability system, a lot of people will still see it as dangerous because it's primarily digital, even if it isn't entirely digital" (U7).

Participants thought effective communication could counter complexity issues and positively impact voter trust. One participant recommended a layered approach that could support a variety of voter information needs: "the way that I've addressed this is to not push a lot into voters' faces immediately, but to make available information so that voters can dig as far as they want" (C3). A usability expert participant commented on the advantages of effective communication: "if you can explain things correctly... and doing that clearly in a way that they understand, will go at least part way to improving trust and confidence" (U6). Several experts said that education for election workers on how to communicate the E2EV process and benefits to voters is especially critical.

Participants also discussed the level of detail needed to achieve the transparency voters desire. Even though E2EV is built on sophisticated mathematics, several experts believed that it is not necessary for voters to understand the details. Although, as previously mentioned, some participants worried that views of E2EV as a "black box" might erode voter trust, one participant thought the abstraction could be advantageous: "You don't have to know what's going on inside. You can look at what happens beforehand, what happens at the end, and see that what happened in the middle must have been right" (C3). Another argued that the transparency voters desire can be achieved by focusing on what E2EV does rather than the technical details, saying, "explaining the math behind the cryptography in [E2EV] is not worth the time for most people. But explaining that at the end of the day, here's how we know your vote was counted as cast is worth the time" (G5).

3) Support for New Voting Technologies: **Several participants suggested that E2EV could enable the introduction of newer and accessible voting technologies.** Towards addressing voters' expectations about the technologies used in elections, participants discussed how E2EV could allow for the use of updated, more familiar technologies in elections. For example, innovations enabled by E2EV could support easier and more accessible voting mechanisms, like electronic ballot return, that could increase election trust and confidence for special populations like voters living outside the U.S. or those with disabilities that prevent them from voting in-person. While participants voiced that electronic ballot return is considered risky from a cybersecurity perspective [15], they thought that E2EV could reduce risk by providing an extra layer of security. An accessibility expert participant reflected: "I think if we use [E2EV] as an opportunity to make people feel more secure about newer technologies, then it could have huge benefits for everyone" (A3).

Despite claimed support for more modernity, several participants noted that current E2EV systems may not be accessible. Participants in accessibility, cybersecurity, and usability expert groups expressed that E2EV has not yet lived

up to its promise of affording accessibility in the voting process: "They haven't figured that out to my knowledge" (U4). Therefore, these systems may "have very limited benefits for people with disabilities" (A3). Participants said this lack of accessibility is typically due to the paper component or other visual verification methods present in most E2EV implementations, which might unwittingly negatively impact "an entire community of voters" (A7), namely visually-impaired voters. Participants further noted that the post-voting E2EV verification process also has to be accessible. Confirmation codes used by voters to verify their vote are typically provided on a piece of paper. However, "from a person with a disabilities perspective, if the code isn't accessible and the verification online, then they're kind of SOL [s*** out of luck]" (A1).

Thus, several participants voiced the need for more to be done to ensure accessibility. A cybersecurity expert noted:

> "anybody who cares about accessibility and true independence has to explore non-paper-based methods to really enable that for meaningful segments of the population. I think that's the thing that I feel is truly missing in this discussion. It tends to focus on security, not access" (C1).

4) Overall value proposition: **Participants were concerned that voters may not see the value of E2EV.** Some participants questioned the value proposition of E2EV for voters as it does not address what participants considered to be the biggest challenges to voter trust and confidence in elections. A cybersecurity expert expressed their concern that E2EV is "a solution in search of a problem" (C2). Several did not think E2EV addresses what they felt voters are most concerned about: ineligible votes. One participant wondered:

> "[W]hat problem are you solving? Because I think if you look at surveys, most people believe that their votes were counted accurately. That is not the issue about where their doubts are coming from. It's not that my vote wasn't counted. It was that other people were able to vote and their votes shouldn't have been counted, or there were lots of extra votes that were added" (U2).

Further, several experts cautioned that centering the value proposition on the added security afforded by E2EV–as it can help identify anomalies in voting systems–might have unintended effects: "as soon as someone has the notion that they should be concerned from a security perspective, that immediately heightens their alarm... You end up losing trust" (C1). Another participant noted, "voting, unlike any other field, is really an area where the voter's perception matters so much. You can build the most secure system in the world, and if voters don't trust it, it doesn't matter" (C6).

Because of the perceived gap between voter concerns and what E2EV currently offers, a participant doubted E2EV would make any impact on voters: "I think putting end-to-end verification on top of already existing systems makes computer scientists feel better. And that's it. I don't think it even makes regular voters feel better because they don't know what it is...I don't think they care" (A3).

Participants voiced that making the value proposition to election officials could be challenging. In a resource-constrained environment, several participants thought election officials would be hesitant to try out a relatively unproven technology. Yet, participants believed that buy-in from "truly innovative election administrators" (C1) who would allow the use of E2EV in their own elections is critical for proving and advancing E2EV. A participant worried that without real-world E2EV deployments, "How are we going to learn how to do it if it's just if we have to do it in an academic paper for two years and then in a lab for two more, and then we release it to the world?" (C1). However, a general election expert noted that election officials may not see the benefit:

> "if election officials can't understand it and explain it, they're not going to use it...The election officials I've talked to about end-to-end ask me all the time, 'What problem does it solve for me?...Am I introducing more problems, or are you solving a problem for me?' " (G5).

To overcome these challenges, participants emphasized that proponents of E2EV must make a better value proposition to election officials, including addressing potential misconceptions about the scale of changes needed to incorporate E2EV into existing voting systems. A participant recommended that technologists:

> "have to get much crisper on both the availability of the technology [and]...the ease by which it can be used with their voting system, right? They [election officials] need to know that I'm not purchasing a whole new voting system because I want to do end-to-end. But in fact, it can be used with the voting system I already have or the voting system I plan to purchase" (G5).

Participants believed that voting system vendors would have to be better incentivized to develop E2EV solutions. In addition to gaining voter and election official interest in E2EV, participants noted that the election vendor community must be convinced to start building E2EV into their voting systems. They expressed that motivation is, in part, dependent on market demand from election officials. Also, several believed that interoperability of E2EV with other voting technologies is a prerequisite for vendor engagement. Participants further commented that the current lack of fully developed E2EV evaluation criteria and processes is another stumbling block for vendors. A cybersecurity expert in the study applauded the inclusion of E2EV in the VVSG 2.0, but noted it will be a challenge "to figure out how to determine whether a system meets those requirements. I think the processes that I've seen so far have not been very effective" (C3) Because E2EV evaluation criteria is not defined, one participant anticipated that it would be a while before an E2EV solution "gets through all of that bureaucracy and gets to the point where it's actually in a polling place and being used" (G7).

Despite value proposition concerns, several participants believed that, if E2EV becomes more widely-implemented, voters and the broader election community will come

to value it. A few participants were optimistic that people will come to accept and trust the technology even if they do not fully understand it. Several acknowledged that there has been demonstrated success of E2EV in smaller, real-world elections, specifically mentioning two ElectionGuard trials. These participants believed that the implementations provided positive proof that E2EV can contribute to or, at the very least, not detract from voter trust and confidence while providing a more secure solution. A participant expressed that, during one implementation they had observed, they did not think E2EV was disruptive: it was "integrated with the process" (C1). In addition, experts relayed that the real-world implementations afforded lessons learned and innovations related to voter communication about E2EV. One participant remarked that during one election, "taking two minutes after the voter voted to explain that they can look up and make sure that their vote was both included in the count and counted as cast went a really long way to their trust" (G5). Another discussed the success of a voter handout that explained E2EV in plain language because it "never says encryption. It never says security. It just says, here's what you can do" (U1).

A few participants believed that voter acceptance can be precipitated not just by demonstration but also by authoritative and trusted messengers and experts who vouch for E2EV as it becomes more commonplace. Two participants used an airplane analogy to explain their optimism. One asked,

> "how many times have you gotten on an airplane? And did you understand what it takes to make an airplane safe?...so why did you do it? Well, you had experts that you believed in, or friends that believed in experts, or experience over time" (C8).

Some participants felt that, while E2EV is "not going to be a silver bullet" (C7) to increase voter trust and confidence, it could be helpful. The majority of participants did not believe that E2EV is the main solution to declining voter trust and confidence. However, several believed that E2EV may appeal to a subset of voters. For example, a participant said, "if there are people who don't have trust and confidence in the ballot casting and counting process, then it will address those... specific concerns that people have" (A2).

A few suggested taking an incremental approach to implementing E2EV in light of the current challenges to widespread adoption. For example, although not fully accessible, having paper ballots as a backup might assuage concerns, as expressed by a participant: "it's crucial in my mind to start with in-person paper ballots with E2E on top of them that will get us used to it" (C8). Another had tempered their original enthusiasm for E2EV over the years, now believing that the elections community should focus on the components of E2EV that realistically could be implemented:

> "I no longer think that we'll have a truly fully end-to-end verifiable voting system where voters can independently verify the entire path. I don't think it's doable at scale...But there are parts of end-to-end verifiable voting that are going to be particularly helpful in locking down how the tabulation works and other things like that" (C6).

Experts recognized that E2EV needs to be part of a multi-pronged strategy and "another tool in the bucket we should be using" (C7) to ensure election integrity and improve voter trust. One participant was unsure about how effective E2EV could be, saying, "I'm not against it. I think adding layers of defense, providing people opportunities to be able to build that trust is a good thing, but it is definitely not the panacea" (G4). A usability expert agreed that E2EV could be just one of several measures for increasing voter trust and confidence in elections: "I think in coordination with your polling place experience or your vote by mail experience, in coordination with other things, I think it does matter" (U1).

Overall, we found conflicting opinions about E2EV. While some participants believed that E2EV has promise for increasing voter trust and confidence in elections, others thought it will be limited in its overall impact or that it might create additional problems for voter trust and confidence.

V. Discussion

Through a first-of-its-kind exploration of election expert perspectives, our findings suggest that, to determine whether E2EV can improve voter trust and confidence in U.S. elections going forward, a holistic approach that addresses the ecosystem of people and processes in elections, in addition to the strength of technology, is needed. In this section, based on our study results (referenced by section), we discuss the potential of E2EV to address major challenges to voter trust and confidence, as voiced by our participants. We then provide suggestions for possible ways to progress efforts towards determining the feasibility of E2EV adoption in U.S. elections.

A. Potential to Address Major Challenges to Voter Trust

> "[E2EV is] this beautiful technical solution to something that I'm not sure is perceived by society as the biggest shortcoming or the biggest challenge with elections right now."
>
> *Participant C2*

From the perspectives of seasoned experts representing different facets of elections, the interviews tell a story of how a combination of challenges—the most pressing of which are not technological—is making it more difficult to engender voter trust and confidence in elections (IV-A). The expert participants further stressed that, while improvements in voting technologies like E2EV may be beneficial, these alone are not sufficient for widely improving voter trust and confidence. Moreover, E2EV was not top of mind for most participants; as discussed in Results, few mentioned E2EV unprompted as a potential improvement for voter trust and confidence.

Given concerns expressed by the participants (IV-C), critical questions remain: Can E2EV address the most pressing challenges election officials face with respect to voter trust and confidence? If not, is further investment in this technology warranted? In this section, we revisit the challenges identified

in our study (IV-A) and discuss how E2EV, as viewed by the participants, has the potential to address those challenges.

Limited or incorrect voter knowledge: The participants predicted that E2EV could introduce additional complexities to an already-complex election ecosystem not well-understood by voters (IV-C2). Lack of voter understanding of verifiable voting processes, albeit in the online voting context, has also been discoverd in prior work [19], [9], [12]. These complexities, if made transparent—for example, the use of sophisticated cryptography or inability to offer remedies if an error is detected—may instigate voter confusion or distrust. To counter confusion, participants recommended carefully crafted communications about E2EV (IV-C1, IV-C2). We also note that, while more than one participant analogized the public's lack of understanding (but acceptance) of airplane technology to E2EV, this analogy may break down at some level. While people many not understand how airplanes work, they still have a fundamental understanding of what they do. This is not necessarily the case for E2EV.

Unrealistic or unmet voter expectations: When first implemented, participants worried that E2EV will introduce changes to the voting process that may challenge voter expectations (IV-C1, IV-C2). Of particular note by participants, E2EV requires a shift in voters' mental models to include a verification step, for if sufficient numbers of voters do not take the verification step, then one of the important properties of E2EV would not be fully realized [5]. While the participants questioned whether voters would be comfortable with the new process (IV-C1) (an issue found in prior work [56], [19], [10], [12]), prior E2EV implementations of ElectionGuard in U.S. elections indicated that, with intentional and professionally-developed voter communications and education, voters generally had a positive voting experience. Additionally, although there are no data on voters' verification experiences in these elections, counts of post-voting accesses to the verifier indicated that a fair amount of voters did indeed take the extra step to check their vote [34], [36], [35].

Diffusion of Innovation (DOI) Theory [57] and prior work on technology acceptance (e.g., [58]) emphasize the importance of trust in the adoption of new technologies. We note that, while an aggregate of voter experiences can impact trust and confidence [7], E2EV addresses just one piece of the voter journey and does not solve problems that voters may be most concerned about (IV-C4), for example, election complexity or ineligible votes being counted. Indeed, recent polls have shown that a majority of voters already feel confident that their own votes are accurately counted at the local level [17], obviating the need for technology like E2EV to provide additional evidence to voters.

The need for usable, accessible, and secure technology: Several participants expressed that E2EV promises enhanced security through cryptographically-verified evidence of the integrity of voting systems (IV-C1), essentially making elections "tamper evident" [59]. None of the participants questioned E2EV's security strengths (in contrast to perceptions of online voting systems [31], [12]). However, even proponents of E2EV acknowledged that accessibility is an important gap in current E2EV systems still needing to be addressed (IV-C3). Further, the usability of the verification process is still in question (IV-C1), especially in light of prior disappointing usability evaluations of E2EV systems [13], [29], [8], [9]. Thus, based on the data, it appears that E2EV currently falls short in its ability to concurrently be usable, accessible, and secure–three technology properties with the potential of influencing voter trust and confidence in voting technologies [56], [20], [7] and encouraging technology acceptance and adoption [57], [60].

Inefficient allocation of election resources: Novel to prior voter-focused research that did not take into account the perspectives of decision makers and influencers in the election space, we were able to identify broader, programmatic challenges to E2EV adoption. With current resource allocations, participants felt that election officials may be unable or hesitant to introduce new technologies like E2EV to their local jurisdictions (IV-A, IV-C4), a concern also expressed in the 2022 E2EV workshop [6]. This hesitation is especially salient since participants expressed that changes to the voting process made by E2EV have the potential to negatively impact voter trust and confidence, thus requiring significant resources to develop effective voter communications and election worker training(IV-C1, IV-C2, IV-C3), as recommended in prior research [19], [10], [12].

Participants posited that E2EV, as a paradigm shift, might be difficult to understand or accept at first, particularly for those who have been working with elections and election technology implementation for a long time. The interviewed experts, who represent the broader election community, demonstrated this uncertainty (IV-B) and skepticism (IV-C). Especially in light of the current lack of E2EV certification, proponents of E2EV may struggle to effectively communicate the value proposition of E2EV to election officials, thus hampering widespread interest and adoption (IV-C4).

B. Moving Forward: Considerations for the Future of E2EV

> "Let's do the research, do studies, and then show the evidence that these things work."
>
> *Participant U4*

While E2EV has the intent of strengthening assurances of election integrity, the future of this technology and its path to widespread adoption is an area needing additional, holistic exploration and research from people, process, and technology perspectives. This study is a start to that exploration. Based on the study results, we offer the following practical considerations and suggestions for future work to assist the election community in determining the path forward for E2EV.

Explore the value proposition for voters. The interviews suggest a need for more research to determine whether E2EV addresses the needs and concerns of U.S. voters (IV-C4). For example, research could explore whether it is enough for voters to know their vote is included or if they would

also want to know their vote was included correctly (which is not possible in E2EV due to the requirement for a secret ballot). Further, more work is needed to gauge whether voters appreciate the public involvement afforded by E2EV, or if other auditing methods (like risk-limiting audits) are enough to garner their trust and confidence.

Explore the value proposition for election officials. The lack of detailed understanding of E2EV among the participants (IV-B) reflects some of the issues inherent in E2EV complexity that would require substantial and careful effort, not just to educate voters, but also to educate election officials and other election community experts with influence on decisions to adopt E2EV voting systems. Therefore, it would be valuable to conduct research about technology adoption needs and the potential of E2EV from the perspective of active election officials representing the variety of types of electoral jurisdictions in the U.S. (e.g., jurisdictions of different sizes and urbanicities).

Research how to best communicate and educate voters about E2EV concepts, benefits, and processes. As suggested by participants, care should be taken when communicating to voters about E2EV, especially when first introduced (IV-C2). This is an area ripe for future research to test communication approaches to see which is most effective with U.S. voters given the complicated election and information environments in the country. For example, future work could explore: how the benefits of E2EV can be transparently described given that cybersecurity may already be confusing or viewed negatively by the general public [61]; if more visibility of security features can increase trust (as suggested in [12] with Swiss voters); which voter concerns may need to be proactively addressed in the communications (e.g., communicating that voter privacy is maintained [9], and, although voters verify their votes online, voting systems are not connected to the internet); what is an appropriate level of detail given that a deep understanding of the technology may not be needed to promote voter acceptance [12]; the efficacy of opportunities for voters to try E2EV systems beforehand (as recommended in [10]); and the role of trusted messengers (akin to change agents in DOI Theory [57]) in promoting voter trust.

Evaluate and address E2EV accessibility and usability issues and their tensions with cybersecurity. To address these concerns (IV-C1, IV-C2, IV-C3), and in light of prior research indicating that voters may be willing to sacrifice usability for security [31], it would be valuable to refresh prior usability research conducted on early E2EV systems (e.g., [13]) to explore modern E2EV solutions and voter perceptions of the balance between usability and security. Importantly, more work is needed to explore accessible alternatives to paper-based methods that provide a chain of evidence accessible to the disability community.

Consider how to enable the development and adoption of innovative technologies like E2EV. While real-world implementations of E2EV were seen as a critical component of learning and prototyping (IV-C4), it may not be prudent to use these as sole proof of production readiness. Rather, if E2EV is pursued in the future, investment in robust and streamlined certification processes would be needed (IV-C4). Additionally, given participants' beliefs that election officials might be hesitant to introduce new technologies (IV-A, IV-C4), introductions of E2EV may need to be incremental, rather than requiring large, sweeping changes [6].

Provide access to researchers. To facilitate quality research exploring the considerations mentioned above, there is a need for more collaboration between election officials, vendors, and researchers. While exit interviews have been helpful to gain the voter perspective in real-world E2EV implementation contexts [35], [36] and voter-specific research has been conducted for online voting in Europe (e.g., [10]), additional research is needed to gain in-depth voter and election worker perspectives for in-person scenarios in the United States. To aid in the collection of reliable data, researchers need more access to modern E2EV systems and experts of those systems. For research outside of a lab, researchers would need access to election officials, polling places, and real-time elections. In turn, researchers can share findings and recommendations related to voting technology usability, accessibility, and communications that may help election officials and vendors.

Encourage increased collaboration between the cybersecurity and election official communities to determine cybersecurity priorities moving forward. Although the cybersecurity participants were split on their opinions about the practicality of E2EV, some participants alluded to a tension between the cybersecurity community's view of E2EV and the needs and challenges of election officials in addressing voter trust and confidence (IV-C4). Additionally, the cybersecurity community has yet to identify solutions to potential issues arising with E2EV adoption (e.g., shortfalls in dispute resolution) [5], [8], [12]. These disconnects warrant constructive conversations between the communities about 1) whether there are higher priority cybersecurity issues for election officials that technologists should focus on instead and 2) what E2EV can and cannot do to address current cybersecurity threats.

VI. Conclusion

Through an interview study of 33 election experts, we uncovered perceptions and thoughts about the potential of E2EV voting systems to positively influence voter trust and confidence. The debate about E2EV was evident in our data. Despite recognizing that technology improvements like E2EV alone would not be a panacea, some participants articulated ways in which E2EV could help address voter trust and confidence, for example, by providing voters with mathematical proof of the integrity of election outcomes that they can check for themselves. However, others articulated concerns that E2EV might introduce additional complexities that could confound the already complex election environment or disengage voters with disabilities or less technology-savvy voters. Thus, the value proposition of E2EV may be in question. These findings provide a holistic perspective towards informing future decisions about investments in efforts that would support wide-scale adoption of E2EV.

DISCLAIMER

Certain commercial companies, products, and participant views are identified to foster understanding, not to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor to imply that these are necessarily the best available for the purpose.

ACKNOWLEDGEMENTS

We would like to thank: the election expert participants who took the time to share their thoughts and experiences with our team; members of the NIST Voting Program for their invaluable input and review; and the anonymous USEC reviewers for their comments that helped improve the paper.

REFERENCES

[1] 107th Congress of the United States of America, "Help America vote act of 2002," https://www.eac.gov/sites/default/files/eac_assets/1/6/HAVA41.PDF, 2002.

[2] U.S. Election Assistance Commission, "Voluntary voting system guidelines," https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines, 2025.

[3] Pew Research Center, "Public trust in government: 1958-2024," https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/, 2024.

[4] Technical Guidelines Development Committee of the Election Assistance Commission, "Voluntary voting system guidelines VVSG 2.0," https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf, 2021.

[5] J. Benaloh, R. Rivest, P. Y. Ryan, P. Stark, V. Teague, and P. Vora, "End-to-end verifiability," 2014, arXiv:1504.03778.

[6] U.S. Election Assistance Commission and National Institute of Standards and Technology, "The path to end-to-end (E2E) protocols for voting systems workshop," https://www.nccoe.nist.gov/get-involved/attend-events/path-end-end-e2e-protocols-voting-systems/overview, October 2022.

[7] C. Stewart III, "Trust in elections," *Daedalus*, vol. 151, no. 4, pp. 234–253, 2022.

[8] K. Marky, O. Kulyk, K. Renaud, and M. Volkamer, "What did I really vote for? On the usability of verifiable e-voting schemes," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[9] K. Marky, M.-L. Zollinger, P. Roenne, P. Y. Ryan, T. Grube, and K. Kunze, "Investigating usability and user experience of individually verifiable internet voting schemes," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 28, no. 5, pp. 1–36, 2021.

[10] K. Marky, P. Gerber, S. Günther, M. Khamis, M. Fries, and M. Mühlhäuser, "Investigating state-of-the-art practices for fostering subjective trust in online voting through interviews," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 4059–4076.

[11] U. Serdült and T. Milic, "Disentangling digital divide and trust: Internet voting affinity in Switzerland," in *International Conference on Electronic Participation*, 2017, pp. 37–52.

[12] M.-L. Zollinger, E. Estaji, P. Y. Ryan, and K. Marky, "'Just for the sake of transparency': Exploring voter mental models of verifiability," in *International Joint Conference on Electronic Voting*, 2021, pp. 155–170.

[13] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach, "Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2014.

[14] R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniue, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora, "Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy," in *USENIX Security Symposium*, 2010.

[15] Cybersecurity and Infrastructure Security Agency, Election Assistance Commission, Federal Bureau of Investigation, and National Institute of Standards and Technology, "Risk management for electronic ballot delivery, marking, and return," https://www.ic3.gov/CSA/2024/240214.pdf, 2024.

[16] M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in internet voting," in *5th International Conference on Theory and Practice of Electronic Governance*, 2011, pp. 1–10.

[17] J. Allen, K. Harbath, R. Orey, and T. Sanchez, "Who voters trust for election information in 2024," https://bipartisanpolicy.org/explainer/who-voters-trust-election-information-2024/, 2024.

[18] M. McArthur, "What makes u.s. elections different: Three observations," https://iall.org/what-makes-u-s-elections-different-three-observations/, 2024.

[19] K. Marky, V. Zimmermann, M. Funk, J. Daubert, K. Bleck, , and M. Mühlhäuser, "Improving the usability and UX of the Swiss internet voting interface," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[20] S. Blahovec, W. Quesenbery, and S. Laskowski, "Voting Technology Series (VTS) 100-2: Training poll workers for accessible voting: Supporting voters with disabilities at the polling place," National Institute of Standards and Technology, Tech. Rep., 2023.

[21] R. L. Claassen, D. B. Magleby, J. Q. Monson, and K. D. Patterson, "Voter confidence and the election-day voting experience," *Political Behavior*, vol. 35, pp. 215–235, 2013.

[22] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press, 2018.

[23] I. Somin, *Democracy and Political Ignorance: Why Smaller Government Is Smarter*, 2nd ed. Stanford University Press, 2016.

[24] O. Bergeron-Boutin, K. Clayton, T. Kousser, B. Nyhan, and L. Prather, "Communicating with voters to build trust in the U.S. election system: Best practices and new areas for research," https://electionlab.mit.edu/sites/default/files/2023-10/voter-trust.pdf, 2023.

[25] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[26] J. C. Benaloh and M. Yung, "Distributing the power of a government to enhance the privacy of voters," in *Proceedings of the Fifth Annual ACM Symposium on Principles of Distributed Computing*, 1986, pp. 52–62.

[27] B. Adida, "Helios: Web-based open-audit voting," in *USENIX Security Symposium*, 2008, pp. 335–348.

[28] B. Adida, O. D. Marneffe, O. Pereira, and J.-J. Quisquater, "Electing a university president using open-audit voting: Analysis of real-world use of Helios," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2009.

[29] F. Karayumak, M. M. Olembo, M. Kauer, and M. Volkamer, "Usability analysis of Helios—an open source verifiable remote electronic voting system," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2011.

[30] B. Romanov, D. D. Cid, and P. Leets, "State versus technology: What drives trust in and usage of internet voting, institutional or technological trust?" *Government Information Quarterly*, vol. 42, no. 4, p. 102068, 2025.

[31] O. Kulyk, S. Neumann, J. Budurushi, and M. Volkamer, "Nothing comes for free: How much usability can you sacrifice for security?" *IEEE Security & Privacy*, vol. 15, no. 3, pp. 24–29, 2017.

[32] C. Burton, C. Culnane, J. Heather, T. Peacock, P. Y. Ryan, S. A. Schneider, V. Teague, R. Wen, Z. Xia, and S. Srinivasan, "Using Prêt à Voter in Victoria state elections," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2012.

[33] ElectionGuard, "Electionguard," https://www.electionguard.vote/, 2025.

[34] ——, "Fulton Wisconsin 2020 special election," https://www.electionguard.vote/elections/Fulton_Wisconsin_2020/, 2020.

[35] ——, "Idaho 2022 general election," https://www.electionguard.vote/elections/Preston_Idaho_2022/, 2022.

[36] ——, "College Park 2023 general election," https://www.electionguard.vote/elections/College_Park_Maryland_2023/, 2023.

[37] S. Fleming, "The inside story of Microsoft's ElectionGuard pilot in Wisconsin," https://news.microsoft.com/on-the-issues/2020/05/13/microsoft-electionguard-pilot-wisconsin/, 2020.

[38] Microsoft, Hart InterCivic, MITRE, Center for Civic Design, Enhanced Voting, InfernoRed Technology, and Oxide, "End-to-end verifiability in real-world elections," https://www.electionguard.vote/images/EAC%20Report%20Final.pdf, 2023.

[39] W. Quesenbery, L. Baumeister, M. Crooks, S. I. Johnson, F. Sanchez, T. Swanson, M. Kropf, E. Mikkelsen, and D. Davies, "Electionguard in College Park city elections in 2023: A report on the implementation

and voter reactions," https://civicdesign.org/wp-content/uploads/2024/01/CCD-ElectionGuard-in-CollegePark-2023-Report.pdf, 2024.
[40] U.S. Election Assistance Commission, "End to end (E2E) protocol evaluation process," https://www.eac.gov/voting-equipment/end-end-e2e-protocol-evaluation-process, 2022.
[41] S. Dzieduszycka-Suinat, J. Murray, J. Kiniry, D. Zimmerman, D. Wagner, P. Robinson, A. Foltzer, and S. Morina, "U.S. Vote Foundation: The future of voting: End-to-end verifiable internet voting - specification and feasibility study," https://www.mobilevoting.org/updates/us-vote-foundation-the-future-of-voting-end-to-end-verifiable-internet-voting-specification-and-feasibility-study, 2015.
[42] U.S. Election Assistance Commission, "Glossary of election terminology," https://www.eac.gov/sites/default/files/glossary_files/Glossary_of_Election_Terms_EAC.pdf, 2021.
[43] A. Regenscheid, "End-to-end (E2E) verifiable protocols for voting systems," https://www.eac.gov/sites/default/files/2023-01/e2e-draft-for-tgdc_508.pdf, 2023.
[44] P. Baxter and S. Jack, "Qualitative case study methodology: Study design and implementation for novice researchers," *The Qualitative Report*, vol. 13, no. 4, pp. 544–559, 2008.
[45] R. K. Yin, *Case study research and applications: Design and methods*, 6th ed. Thousand Oaks, CA: Sage, 2018.
[46] H. Kim, J. S. Sefcik, and C. Bradway, "Characteristics of qualitative descriptive studies: A systematic review," *Research in Nursing & Health*, vol. 40, no. 1, pp. 23–42, 2017.
[47] M. Sandelowski, "What's in a name? qualitative description revisited," *Research in Nursing & Health*, vol. 33, no. 1, pp. 77–84, 2010.
[48] R. E. Stake, *The Sage handbook of qualitative research*, 3rd ed. Sage Publications Ltd., 2005, ch. Qualitative Case Studies, pp. 443–466.
[49] P. Fusch and L. R. Ness, "Are we there yet? data saturation in qualitative research," *Walden Faculty and Staff Publications*, p. 455, 2015.
[50] U.S. Department of Justice, "Election threats," https://www.justice.gov/archives/voting/election-threats, 2024.
[51] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.
[52] ——, "Conceptual and design thinking for thematic analysis," *Qualitative Psychology*, vol. 9, no. 1, p. 3, 2022.
[53] R. S. Barbour, "Checklists for improving rigour in qualitative research: a case of the tail wagging the dog?" *British Medical Journal*, vol. 322, no. 7294, pp. 1115–1117, 2001.
[54] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice," in *Proceedings of the ACM on Human-Computer Interaction*. ACM, 2019, p. 72.
[55] C. A. Barry, N. Britten, N. Barber, C. Bradley, and F. Stevenson, "Using reflexivity to optimize teamwork in qualitative research," *Qualitative Health Research*, vol. 9, no. 1, pp. 26–44, 1999.
[56] S. Agbesi, A. Dalela, J. Budurushi, and O. Kulyk, "What will make me trust or not trust will depend upon how secure the technology is: factors influencing trust perceptions of the use of election technologies," in *Seventh International Joint Conference on Electronic Voting*, 2022, p. 1.
[57] E. M. Rogers, *Diffusion of Innovations*, 5th ed. New York, NY: Free Press, 2003.
[58] K. Wu, Y. Zhao, Q. Zhu, X. Tan, and H. Zheng, "A meta-analysis of the impact of trust on technology acceptance model: Investigation of moderating influence of subject and context type," *International Journal of Information Management*, vol. 31, no. 6, pp. 572–581, 2011.
[59] C. Duffy, "Microsoft hopes its technology will help Americans trust voting again," https://www.cnn.com/2020/02/22/tech/microsoft-election-guard-voting-test/index.html, 2020.
[60] L. F. Cranor, *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc., 2005.
[61] A. von Preuschen, M. C. Schuhmacher, and V. Zimmermann, "Beyond fear and frustration-towards a holistic understanding of emotions in cybersecurity," in *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, 2024, pp. 623–642.

APPENDIX A: INTERVIEW PROTOCOL

NOTE: The interview protocol for each expert group was similar, with slight changes to emphasize the area of the expertise. The following is the interview protocol used for cybersecurity expert participants.

I'm [name] from [institution]. We're conducting research interviews with election cybersecurity experts like yourself about your perceptions of challenges in voting, and potential impacts to voter trust and confidence in elections ahead of the 2024 election. We're interested in your views from the election cybersecurity perspective.

Before we begin the interview, I'd like to review a few key points covered in the information sheet we provided you earlier, see if you have any questions, then get your verbal consent to participate in the study.

- The interview should take about an hour. Every question is voluntary – you can decline to answer any question or to end the interview at any time. At the end of the interview, we'll ask you if there is data that you wish to remove from the research record. You also have up two days after today to request anything be removed or to withdraw from the study, at which time all your data will also be withdrawn.
- The interview will be audio and video recorded. After that, the audio will be professionally transcribed. To facilitate the conversation, we strongly encourage you to keep your camera on during the interview.
- The recording and the transcript will not be labeled with your name, rather given an anonymous participant identifier to protect your confidentiality. Also, any reports we eventually issue about this study will report results in aggregate and keep your identity confidential.
- All of your data will be stored on secured [institution] computers or servers or in a locked office. The recording and links to your name and contact information will be destroyed at the conclusion of our study.
- During the interview, we ask that you try not to mention identifiable information such as people's names or your organization's name to protect confidentiality. However, if you do mention that type of information, we'll redact it from the transcript.

Do you have any questions about any of that?
Do you agree to be recorded and participate in the study?

I'll start out with a few questions about yourself and your expertise, then we'll talk about your thoughts on current and future challenges in voting. Ready? I'll start recording now.

[Start recording. Say date, time, and participant ID.]

1) Please describe your background and current role with respect to elections.
   a) How long have you been involved with cybersecurity related to elections?
2) From your perspective as an election cybersecurity expert, can you describe the biggest challenges to voter trust and confidence in elections today, if any?
   a) *[If participant does NOT talk about election outcomes]* Can you talk about challenges with voter trust and confidence, if any, related to **election outcomes**?

b) *[If participant does NOT talk about technology]* Can you talk about any **technological challenges** that may exist with voter trust and confidence in elections?
c) *[If participant does NOT talk about election support technology]* Can you describe any challenges, if any, with voter trust and confidence related to other **technologies that support elections**?
d) *[If cybersecurity expert does NOT talk about cybersecurity]* What about **cybersecurity**?
e) *[If participant ONLY talks about technology]* What about **non-technological challenges** with voter trust and confidence in elections?
f) Out of everything we've discussed so far, what do you think are the **top 3 most pressing issues** in elections today and why?
g) Why do you think these haven't been addressed in the election community?
h) *[If participant does NOT talk about underlying causes]* What do you think are the **underlying causes** of challenges to voter trust and confidence in elections?

3) From your perspective as a cybersecurity expert, how can voter trust and confidence in elections be **improved**?
a) *[If participant does NOT talk about technology]* What **technology** could improve voter trust and confidence?
b) *[If participant ONLY talks about technology]* What about **non-technological** improvements?
c) *[If participant does NOT talk about the needs of election officials]* How can election officials be better supported to address challenges with voter trust and confidence in elections?

4) Thinking further into the *future*, say well beyond the 2024 election, do you think some of the challenges you previously noted, such as [challenges participants mentioned] will still be around? *[If asked, specify at least 10-15 years in the future]*
a) Why do you think that is?
b) What new challenges to voter trust and confidence in elections, if any, might exist in 10-15 years?
c) What technologies do you believe will be the *future* of elections?

5) Are you familiar with the concept of end-to-end-verifiable voting systems (E2EV for short)?
a) *[if no, skip to last question]* That's ok, most people aren't because it's not widely adopted yet. E2EV systems are software independent voting systems that are an alternative to the traditional paper-based voting systems. Unlike paper-based voting systems, E2EV voting systems have the ability to allow voters to verify that their vote was cast as intended and tallied as cast. The reason we asked is because we are interested in whether people think this technology might increase voter trust and confidence in elections. If you want more information, we can send you some links to learn more about E2EV.
b) *[if yes]* In your own words, can you briefly describe what an E2EV voting system is?
i) *[if description isn't related to E2EV voting systems, skip to last question]* Thank you.

6) *[if description is close to E2EV, or if they name one of the E2EV voting systems]* How do you think E2EV systems might impact voter trust and confidence in elections, if at all?
a) What, if any, do you think are the benefits of using an E2EV voting system?
b) What, if any, do you think are the challenges of using an E2EV voting system?

7) Any other thoughts you'd like to share related to our discussion today?

Great! I'll stop the recording now. Thanks so much for participating in this interview and providing your perspective!

Is there anything that you mentioned during the interview that you'd like us to remove from the research record?

Should you have any issues or questions afterwards, our contact information is on the information sheet. Thank you again!

APPENDIX B: CODEBOOK

The following table describes the codes used to inform this paper.

TABLE I: Interview Codebook

PARENT CODE Sub-code	**Operationalization**	**Example**
ACCESSIBILITY	Expression of concepts pertaining to accessibility in elections and the community of voters with disabilities; assistive technology or processes that support voters with disabilities.	"how is the providing of that [E2EV verification] code going to be accessible? That's going to be a real challenge." (A1)
CHALLENGES	Challenges may be non-adversarial (such as limited funding or personnel), adversarial (such as those posed by hackers), technological, or non-technological.	"when you introduce a new technology, you also introduce new questions and new challenges for users as well as for observers." (U3)
Complexity	References to the complicated nature of elections, including their varied and dispersed processes, policies, and technologies. May also refer to the inherent complexities of software and technology in general.	"building verifiable technologies includes a lot of mathematics that most people are not going to understand." (C3)
Tension	Mention of strain or tradeoffs between opposing concepts or communities, for example, accessibility and cybersecurity (security), academics/researchers and election officials.	"that's where my concern...comes into place. It's when we subvert accessibility to promote security when, in fact, we should be doing both" (A7)
CHANGE	Expressions of the ways in which technology, processes, and people evolve. Change can be positive or negative, rapid or slow. Can include references to lack of change.	"Maybe it's good that elections move slowly, right? I mean, work fast and break things is not what we want in elections." (U1)
Future	References to the ways in which elections may or may not change going forward, including technology and process used, challenges faced, etc.	"I think the other thing you're going to see in 10 to 15 years is building on that concept of auditability of the results" (G5)
Improvements/advancements	Mention of anything that has the potential to improve elections, including solutions or methods to increase voter trust and confidence. May be technological or non-technological.	"I think vendors can do more in terms of transparency, can provide documentation, educational materials." (C6)
COMMUNICATIONS & EDUCATION	Expressions of the needs, challenges, and current state of communicating with voters, election officials, experts, etc. This also includes outreach that is intended to facilitate voter education of election methods and processes.	"I think maybe that's how you increase voter trust and confidence, is just increasing the knowledge of what election processes look like. " (A2)
CYBERSECURITY	Expression of concepts pertaining to cybersecurity in elections, like: confidentiality, integrity, and availability of data; network protection and intrusion detection; website security; data privacy and data protection; vulnerabilities; Excludes physical security, safety, and personal security.	"the more you talk to people about the security procedures that are in place in our system, the more confident they feel that they can trust it" (U2)
E2EV	Responses about end-to-end verifiable voting systems, including level of familiarity, definitions, benefits, challenges, and perceptions on possible impacts to voter trust and confidence arising from E2EV systems.	"I'm also a fan of end-to-end verifiability" (C8)
Description	The participant's response when asked to describe E2EV in their own words.	"it's ensuring that the vote cast is the vote counted and received. Is that you have created a system where you're fully confident in whoever you voted for is the intended result, and that there isn't any break in the process." (A2)
Impact	The participant's response when asked if E2EV will have an impact on voter trust and confidence; this includes any benefits or challenges mentioned by the participant.	"It's a great solution to a hard problem, but it's just not a thing that most people are going to be motivated to try to wrap their head around." (U5)

TABLE I: Interview Codebook

PARENT CODE Sub-code	**Operationalization**	**Example**
ELECTION METHODS & PROCESSES	Encompasses all election-related processes, from early and in-person voting, to military and oversees voting (UOCAVA), to voter registration and election support systems. Methods and processes may be technological or non-technological. May include statements of fact about elections and the overall voting landscape in the U.S.	"I think the sort of mechanics of elections are complicated. They're complex. There's a lot of systems at play that allow elections to function." (G8)
Voting technology	Election technology used by voters and/or election personnel to mark, cast, or tally their votes, which can include, paper ballots, direct recording electronic voting machines (DREs), electronic ballot marking devices (BMDs), internet/online voting etc. Election technology can also encompass election supporting technology (e.g., e-poll books, voter portals, voter registration databases). This can refer to general technology used in support of elections (e.g., tablets, computers, websites). This includes mentions of voting system vendors.	"I think it [technology] can be extremely useful, both in increasing and improving participation and increasing and improving confidence in the system, which I think is kind of critical for the system to work." (U2)
Success stories	Kudos to election practices of local or state jurisdictions, or federal efforts. Success stories may be technological or non-technological.	"It appears that the county of [county name] is really the leader in creating a more universal design kind of system." (A4)
ELECTION PERSONNEL	Responses about the needs, challenges, perceptions, or education of professionals who work in elections. Personnel may be paid (election officials) or unpaid (poll workers).	"that's another good way, just to have, again, these groups that are getting that information out. And nationally, I think organizations like National Association of Secretaries of State– the Secretaries get out there and speak." (G6)
Election officials	Professionals who work in elections. Distinct from volunteers, typically paid staff.	"election administrators tend to be very transparent about what they do." (C6)
Poll workers	Members of the general public who support elections in polling places. They are typically volunteers trained to do things like opening the polls, checking in voters, and helping run the polling place on election day. This is distinct from election officials who are professionals rather than seasonal election staff.	"make sure that those who are observers, those who are poll workers, those who understand what's actually happening, are able to communicate that message." (G7)
INFORMATION ENVIRONMENT	References to widespread availability of information related to elections, including information overload. Can include references to the larger information ecosphere and a variety of sources including local connections, news, media, online, social media, etc.	"We're in an environment where there is such information overload." (G4)
PRIVACY	References to the lack of secrecy of an individual's vote/ballot. This does not include references to the privacy of voters or other individuals themselves.	"for people with those kinds of disabilities that impact their ability to vote privately and independently in the traditional ways, most of them, now, in 2024, rely on technology." (A1)
USABILITY	Expression of concepts pertaining to voter and poll worker experiences relevant for elections that focuses on efficiency, effectiveness, and satisfaction.	"There are a variety of parts in lots of different voter's voting experience that can be somewhat complicated, either from a cognitive intellectual standpoint or from a physical ability to complete the task standpoint." (U7)
VOTERS	Any reference to voters, including those who actively vote or are eligible to do so. Includes their perceptions, tasks, needs, or challenges. Note: references to generic "people" often refers to voters in these interviews.	"my thoughts go towards specialized systems to support small populations of those in great need to vote by mail." (C2)

TABLE I: Interview Codebook

PARENT CODE Sub-code	**Operationalization**	**Example**
Expectations	Mentions of voters' strong beliefs or assumptions that something should happen or is happening. Includes expectations about the stability or reliability of election technology. Can include concepts like accessibility and interconnectivity. Includes analogies like mobile banking.	"As people become comfortable with a particular technology, then they would want to apply that to more aspects of their life. " (G6)
Influence on trust and confidence in elections	Responses related to what has an impact on voter trust and confidence, either negative or positive. Also includes any abstract expressions of voter trust and confidence.	"I hear all the time from election officials that they hear from voters who don't have confidence, and they invite them in, and they give them a tour, and they ask them to participate, and everything turns around." (C8)
Knowledge and understanding	Mentions of voters' actual understanding, or lack thereof, related to voting and elections. Includes perceptions, actual or perceived knowledge, and mental models.	"differing processes, differing technologies, differing terminology creates this opportunity for confusion." (G4)

APPENDIX C: ETHICS

1) Stakeholders and Potential Impacts: Because of the sensitivity of U.S. elections and the relatively small community of election experts in each of the four areas of interest, participant confidentiality could be at risk, a breach of which could result in reputational harm. Additionally, the research team could come under increased scrutiny.

Our study results could potentially impact decisions made by local, state, and national election administrators and support organizations about future investments in E2EV solutions. If investment is ultimately deemed untenable, this may have a negative impact on financial opportunities for researchers and industry developers of E2EV solutions. From a positive perspective, curtailment could result in election-based public and private organizations shifting their focus to technologies or solutions that address other pressing issues related to voter trust and confidence. Alternatively, should future investment in E2EV systems be recommended, our study findings could result in more efforts to improve the usability, accessibility, and communications surrounding E2EV solutions, making for a more positive experience for voters and election workers.

2) Mitigations: Our institution's research protections office (institutional review board) determined that the study protocol met the criteria for "exempt human subjects research" as defined in the U.S. Common Rule for the Protection of Human Subjects. To mitigate potential harms to stakeholders and ensure adherence to ethical research principles, we took the following measures when designing, executing, and reporting our research.

Consent and voluntary participation: Participation in the study was voluntary and involved a consent process. To protect participant confidentiality, we did not collect signed informed consent documents that could link individual experts to the research. Instead, several days prior to data collection, we provided participants with an information sheet detailing the study purpose, potential contributions and benefits of the research, potential risks for participating in the study, and how their data and confidentiality would be protected. In the beginning of our virtual meetings (prior to asking the interview questions), we reviewed the information sheet with participants and answered any questions they had. The expert participants then provided explicit, verbal, informed consent to participate and be recorded. To mitigate the potential risk of participant discomfort if they felt that their responses to questions may be sensitive in nature or embarrassing, responses to all questions were voluntary. At the end of the interview, we asked participants if there was anything they said that they would like to be removed from the research record. Participants also had the option to withdraw from the study or redact parts of their interview at a later time. None of the participants withdrew or requested redactions.

Participant references: We do not include individual participant demographics in this paper; rather, we report participants' expertise in aggregate. We assigned an anonymous reference code for each participant (e.g., G8). We also selected quotes for use in the paper which did not reveal identifiable information. We asked participants not to mention their participation in the study to others; however, we cannot guarantee that they adhered to this request.

Data management: We redacted data from the interview transcripts that could be linked back to the participants, their organizations, or other election experts. After the completion of data analysis, per our approved study protocol, we deleted all research records that could be used to identify our participants, including: emails to/from and about prospective participants; calendar invitations; interview recordings; unredacted transcripts; and lists of potential participants. Remaining data–to which only approved researchers have access–are stored on secured server platforms approved for this use in accordance with our institution's research records retention policy.

Multiple perspectives: To obtain balanced perspectives on E2EV, we recruited participants from multiple stakeholder groups in different expert areas and included those from: local, state, and national government; nonprofit election organizations; academia and research institutions; and election vendors. Together, the participants broadly represented the concerns of U.S. voters, election administrators, and election technologists. Recognizing the dichotomony of the experts' opinions on the feasibility of widespread E2EV adoption, we aimed to fairly report all perspectives in this paper.

Ensuring Research Validity: We put in place mitigations to counter any potential question of the research team engaging in trustworthy and credible research. The team's interdisciplinary nature and our systematic methodology allowed us to recognize and address potential predispositions or partialities of team members at every step. Also, the study protocol and this paper underwent a rigorous review and approval process within our institution. The process included multiple and iterative technical, writing quality, ethical, and policy reviews conducted by voting technology experts and program managers, ethical research experts, senior leaders, and communication coordinators.

3) Decision to Conduct and Publish Research: Given the inclusion of E2EV as a possible solution in VVSG 2.0, decisions on E2EV investment were made at the local, state, and national levels soon after study completion. Therefore, it was deemed important by external stakeholders in the election community that we conduct the study and publish findings as expeditiously as feasible, with potential benefits outweighing any risks in consideration of the mitigations we enacted.