JeDEM Issue 16 (3): 1-28, 2024
ISSN 2075-9517
http://www.jedem.org
Date of submission: 30.04.2024
Date of acceptance: 30.09.2024
Article DOI: 10.29379/jedem.v16i3.916

Investigating transparency dimensions for internet voting

Samuel Agbesi

ORCID Nr: 0000-0002-9527-1924
Niels Brock Copenhagen Business College, saag@nielsbrock.dk

Jurlind Budurushi

ORCID Nr: 0000-0002-6732-4400
Baden-Wuerttemberg Cooperative State University, jurlind.budurushi@dhbw-karlsruhe.de

Asmita Dalela

ORCID Nr: 0009-0004-4031-161X
asmita.dalela@gmail.com

Oksana Kulyk

ORCID Nr: 0000-0003-4218-1658
IT University of Copenhagen, okku@itu.dk

Abstract: While internet voting is argued to have the potential to improve election processes, concerns about security risks remain one of its main adoption barriers. These concerns are furthermore aggravated by the lack of transparency of internet voting systems that are often perceived as a "black box". Moreover, there is a research gap in conceptualising transparency and studying voters' attitudes towards transparency in internet voting. In this work, we aim to address this gap by (1) Conducting a systematic literature review, from which we identified five dimensions of transparency; (2) Developing a questionnaire (Transparency Dimensions of internet voting, TDIV) to assess voters' attitudes regarding the correlation of these dimensions with transparency; and (3) Conducting an online study (N=500) to investigate voters' attitudes to-

wards transparency in internet voting. We conclude that providing information about the security of the internet voting system, testing it by independent experts for security vulnerabilities prior to the election, monitoring the election process and verifying its integrity, and providing a remedy for security breaches while holding the responsible parties accountable, are perceived by voters as necessary, and enhance transparency in internet voting systems.

Keywords: internet voting, i-voting, electronic voting, e-voting, transparency, user study

Acknowledgement: This work was supported by a research grant (40948) from VILLUM FONDEN.

1. Introduction

Internet voting has been an active topic of public discussions for many years, with its proponents pointing at the advantages of being able to cast one's vote over the internet as increased convenience and accessibility, e.g. by accommodating voters unable to get to a polling station physically. On the other hand, criticism of internet voting has pointed at issues such as its security risks, e.g. the possibility of manipulating election results or violating vote secrecy. Addressing these risks and ensuring voters' trust in the system's security is particularly challenging, given the complexity of internet voting systems and corresponding security measures.

Transparency, as providing a means for the public to follow the workings of the voting system and ensure that the election has been conducted according to proper procedures, becomes a significant and essential factor in establishing trust, as confirmed by multiple studies (Agbesi et al. 2022; Marky et al. 2022; Faraon et al. 2015), and acknowledged by the decision of the German Constitutional Court regarding the use of voting machines (Federal Constitutional Court of Germany 2009). However, while several technical measures have been proposed to improve the transparency of voting technologies (Nurse et al. 2017; Saldanha and Silva 2020), limited attention has been dedicated to studying voters' attitudes towards transparency in internet voting in general, as well as towards the proposed measures and the extent to which they are perceived as being related to transparency.

In this work, we aim to bridge this gap and investigate voters' attitudes toward the transparency of internet voting. Our study investigates the following research question: *What measures can be used to increase transparency in internet voting systems as proposed in academic research and applied in practice, and what are the voters' attitudes towards these measures and their relation to transparency?*

Our contributions are the following[1]:

- We conduct a systematic literature review on measures proposed to improve transparency in internet voting. We propose a taxonomy of these measures by deriving five dimensions: namely, information availability, understandability, monitoring and verifiability, remedial measures and testing. These differ depending on the involved stakeholders, the time period when these measures are applied (e.g. before or during the election) and their effect.

[1] A shorter version of this paper was published and presented at the E-Vote-ID conference in 2023.

- Based on the taxonomy, we develop and empirically validate (N = 50) a questionnaire which we call "Transparency Dimensions of Internet Voting" (TDIV), which is designed to measure voters' assessment of the five dimensions of transparency in internet voting systems as well as transparency in general (as overall attitudes and as related to specific systems)
- We conduct an online user study (N = 500) by applying the TDIV questionnaire in order to study voters' attitudes towards the measures across the five transparency dimensions and transparency in general. In particular, we conduct a quantitative analysis studying the relationship between the perceived importance of individual dimensions and the perceived importance of transparency in internet voting in general.

Our findings show that voters' perceptions of four out of five proposed di- mensions (namely, information availability, monitoring and verifiability, remedial measures, and testing) indeed correlate with their perceptions of transparency in internet voting in general. On the other hand, our study shows mixed effects of understandability of the voting system; while some participants mentioned the importance of being able to understand how the system works, we did not find a significant correlation between the attitudes towards understandability and attitudes towards general transparency, indicating the need for future investigations to understand the relationship between these two concepts better.

2. Literature review

We describe the systematic literature review conducted to define the concept of transparency and identify its different dimensions as well as the proposed hypothesis. We used the following search phrases: *("Transparency" OR "TRANSPARENCY" OR "Openness" OR "Understandability") AND ("internet voting" OR "INTERNET VOTING" OR "E-VOTING" OR "E-voting" OR "Online Voting" OR "Remote Voting")*. We manually searched databases such as Springer, IEEE, Scopus, Web of Science, ProQuest, and Emerald Insight. We also looked into research publications in the proceedings of the E-Vote-ID conference2, one of the leading conferences dedicated specifically to electronic voting. Two paper authors evaluated the publications for their relevance to the research inquiry. Our inclusion criteria considered publications published between 2015 and 2022 on transparency, as well as empirical and theoretical papers. Technical papers, non-empirical papers, papers that did not discuss transparency and trust, and papers that were not written in English were all excluded. We reviewed the abstracts of the remaining papers and eliminated those that were not relevant to the research topic or aims. Finally, the snowballing approach (backward snowballing) was used in reviewing the papers. The authors used this method by reviewing the reference list of the initial set of

2 https://e-vote-id.org, last accessed on 09.02.2023

papers extracted and selecting additional relevant papers, which were then added to the list. The review included a total of 14 papers in total that focus on transparency in election technologies3.

Based on the reviewed papers, the five main dimensions, *Information Availability, Understandability, Monitoring and verifiability, Remedial Measures*, and *Testing,* were identified through an iterative discussion process.

In the following subsections, we describe the results of our literature review. We then elaborate on our conceptualisation of transparency in internet voting, describe the five identified dimensions of transparency and provide the hypotheses related to these dimensions that inform our follow-up studies.

2.1. Transparency in election technologies

At the time of writing, only a few studies have investigated transparency in the context of election technologies, such as electronic voting. For instance, Driza Maurer (2019) reviewed how to develop systems that increase transparency to improve voter confidence by identifying design requirements such as verifiability, public intrusion testing, and source code publication. Buckland, Teague and Wen (2011) discovered that little information about the Australian electronic voting system was available and that the source code and technical documentation were not publicly available. The authors conclude that the lack of transparency negatively influenced voters' attitudes toward electronically held elections. Note that one of their key recommendations is that source code, technical documentation, user and training manuals, and audit reports should be made public. Volkamer, Spycher and Dubuis (2011) concluded that transparency in election technologies is key to voters' overall trust and could positively influence voters' behaviour towards electronic voting. While these studies have looked at transparency in electronic voting systems, they did not fully examine the various dimensions of transparency: that is, there is a lack of research for conceptualising transparency. Saldanha and Silva (2020) attempted to identify the transparency characteristics in the Brazilian electronic voting system but failed to investigate the significance of these characteristics and how they influence transparency. We complement their work by conceptualising transparency and examining the importance of its various dimensions for voters in the context of internet voting.

2.2. Conceptualisation of transparency

Transparency has been defined as the process of ensuring that a system is open and externally accessible to the public (Song and Lee 2016), as well as the availability of information about the election system and the actors (Fragni`ere et al. 2019). Jain and Jain (2018) also argued that transparency concerns information disclosure and openness. Studies have also shown that a transparent election system is one that supports the verifiability of votes, observation and monitoring (Nurse et

3 We discuss relevant papers on transparency related to other domains in information technology in section 5

al. 2017), accountability, as well as public oversight, and comprehension of the election process (Hall 2006). Furthermore, Saldanha and Silva (2020) also identified several transparency characteristics in election technology, including consciousness, accountability, explanation, testing and auditing. As a result, in the context of our work, transparency is defined as having characteristics such as information availability, understandability (explainability), monitoring and verifiability, remedial measures, and testing (Hall 2006; Nurse et al. 2017; Song and Lee 2016, Fragni`ere, et al. 2019; Saldanha and Silva 2020), which are further elaborated in the following sections.

Information Availability refers to the ability to make information about the election system, specifically the internet voting system, available to relevant stakeholders (Driza-Mauer 2019). This information could include source code, technical documentation, vendor information and user manuals (Driza-Mauer 2019; Fragni`ere et al. 2019). It is important to emphasise that information availability about internet voting has been argued to influence transparency (Driza-Mauer 2019; Hall 2006). Hall (2006) argued that even if voters do not understand the source code, its availability may increase transparency. Once the source code is published, experts can review it for any hidden bugs. Note that the level of accessibility of the provided information can vary: as such, some of the information can be made available either publicly or upon request only; similarly, some of the information, such as technical documentation, might require a relatively high level of expertise to understand it.

Understandability is the ability to explain how the system works and in particular, given the concerns about security risks of internet voting, the extent to which system security is guaranteed. The explanation, moreover, needs to be done in such a way that a layperson can understand. Note that while this category is similar to information availability in terms of providing information about the workings of the voting system, the important distinction is that measures aimed at understandability imply that everyone, as opposed to just the experts, can understand the provided information. For example, Saldanha and Silva (2020) found that explaining the algorithm and security protocols, as well as how the system works, can positively influence voters' attitudes toward transparency. Similarly, "understandability" was identified as a characteristic of transparency in the work of Spycher et al. 2011.

Monitoring and Verifiability refer to various measures implemented during or after the election to ensure that the election processes run according to a proper procedure. In particular, end-to-end verifiability has been widely advocated for by election security experts as a means to detect election manipulations, proposing techniques that enable voters to verify that their vote has been correctly cast, stored and tallied (individual verifiability) as well as techniques that enable the general public to verify that the stored votes have been tallied correctly (Nurse et al. 2017; Puiggali et al. 2017). Other methods to ensure the correctness of election processes include non-technical measures such as ensuring that independent parties observe the important steps of voting and tallying. According to Solvak (2020), the availability of a vote verification process increases voters' confidence that their vote was cast correctly. To improve transparency, many electronic voting system implementations have included verification processes. Puiggali et al. (2017), for example, identified countries such as Norway, Switzerland, Estonia, and Australia implementing some form of verifiability in their electronic voting system to increase transparency.

Remedial Measures are various methods for dealing with situations in which something goes wrong, including security breaches as well as other issues that might jeopardise the integrity of the election. This includes both error-correction measures and accountability measures that allow for the identification of individuals or entities responsible for these errors (Saldanha and Silva 2020). Hence, voters, for example, may perceive an internet voting system as transparent if the system can detect errors or breaches, implement corrective measures, and identify the entities responsible for these breaches.

Testing refers to the various measures taken prior to the election to ensure that the internet voting system is sufficiently secure. This includes code review measures, public intrusion tests, formal verification, and other auditing-related measures, in particular measures allowing the general public to participate in the testing and resolution of any discovered vulnerabilities, which can improve transparency (Saldanha and Silva 2020, 10, Portes, N'goala and Cases 2020).

2.3. Hypotheses

Given the identified dimensions of transparency in internet voting, we conduct an empirical evaluation in order to understand whether these dimensions are indeed perceived as related to transparency by voters. In doing this, we follow an indirect approach of studying whether the perceived importance of any of the dimensions is correlated with the perceived importance of transparency. Such an approach allows us to investigate voters' attitudes independent of a particular voting system, which is beneficial when studying the attitudes of populations that did not yet have experience with voting online. We therefore define the following hypotheses:

H1: There is a positive correlation between the perceived importance of information availability and voters' attitudes towards transparency.

H2: There is a positive correlation between the perceived importance of under- standability of the internet voting system and voters' attitude towards transparency.

H3: There is a positive correlation between the perceived importance of verifiability of the internet voting system and voters' attitudes towards transparency.

H4: There is a positive correlation between the perceived importance of remedial measures and voters' attitudes towards the transparency of the internet voting system.

H5: There is a positive correlation between the perceived importance of testing and voters' attitudes towards the transparency of the internet voting system.

3. Methodology

This section describes the methodology for developing and evaluating the questionnaire, as well as for the study conducted using the questionnaire to investigate the defined hypotheses.

Our goal when developing the questionnaire was two-fold. First, we wanted to propose an instrument that can be used in future studies to evaluate voters' perception of each transparency dimension with respect to any internet voting system (e.g. whether the voters believe that the system provides sufficient information, that is, the extent to which information availability is ensured). Second, we wanted to understand the relations between individual dimensions of transparency and their related measures, as well as the perceived transparency in general.

As currently, very few countries have implemented internet voting for legally binding elections, we assumed that our questionnaire would target mostly people who do not have a particular system in mind when asked about internet voting. Nevertheless, our questionnaire can also be applied to people who have used internet voting in order to measure and improve the transparency of the corresponding system.

3.1. Questionnaire development and testing

Development of the TDIV Items: The TDIV instrument consists of the following dimensions (also known as variables or constructs): Information availability, Understandability, Monitoring and verifiability, Remedial measures, Testing and Transparency. Based on the literature review and our internal discussion, we added at least four (4) closed-ended questions or items to each variable of the TDIV instrument4. Each item consisted of a statement about the importance of a transparency-enhancing measure related to a corresponding transparency dimension (e.g. "The documentation on how the internet voting system works should be available to the public" for information availability) or transparency in general (e.g. "Transparency is an integral aspect of internet voting system") similar to the TVS questionnaire (Acemyan et al. 2022) with the responses measured using a 7-point Likert scale (1- Strongly disagree to 7- Strongly agree).

Validation of the TDIV: To ensure the validity of our TDIV instrument, we conducted a face-to-face validation check (Aithal and Aithal 2020). Thereby, we asked three experts (cryptography, election technology and security) to examine the various dimensions or variables and items of transparency. The experts were required to determine any ambiguities or inaccuracies and check if the items addressed the research questions. The opinions and ideas of the experts were used to update the dimensions and question items. After the first validation, in order to evaluate that the various transparency dimensions and their items are easy to understand, we conducted a pilot study with a small number of respondents (sample size of 50, that is 10 per cent of the sample size for the main study (500) (Aithal and Aithal 2020)). The pilot study enabled us to adapt the transparency dimensions and their question items when we detected that the respondents had difficulties understanding them (Aithal and Aithal 2020). Based on the results of the pilot study, we slightly adjusted several of the

4 The resulting variables are available at https://github.com/comet-itu/constructs/blob/main/Codes_constructs.pdf

items and removed some of them. We detected these difficulties through the open-ended questionnaire, where we explicitly asked if the participants encountered any issues in the pilot study5.

3.2. Study procedure

Our study applying TDIV has been conducted as an online survey using the SoSci Survey platform6. We recruited the participants for our survey from the Prolific7 platform. The participants were recruited from the US, UK, Estonia, Denmark, Sweden and Norway.

To reduce the bias that comes with online surveys like prolific, we conducted a pilot test with a small group of respondents before administering it to a larger population. It helped us identify any potential issues with the survey. We furthermore used the option to recruit a gender-balanced sample, which, according to previous research, is reasonably representative of the general population with regard to security and privacy-related research (Redmiles et al. 2019). Each participant received 1.5 UK pounds sterling in compensation for an estimated 10 minutes of participation, which corresponds to the recommendation of the Prolific platform. Following the recommendation by Aithal and Aithal (2020), we aimed to recruit a total of 500 participants. In order to control for the quality of the responses, we included attention checks in the survey, namely, two Instruction Manipulation Checks (IMC) (Oppenheimer et al. 2009). In terms of voting experience, most of the participants (59%) did not have any experience with internet voting, and only 16% had experience ranging from good to excellent.

At the beginning of the survey, the participants were provided with information about the study and asked to provide their consent for participation. Then, they were asked about their previous experience with internet voting, presented with a hypothetical scenario where they were asked to imagine that their country wants to implement internet voting for the next elections and asked whether they would be willing to vote online in such a scenario. They were then presented with the items from the TDIV questionnaire. For each one of the dimensions, the participants were asked an additional open-ended question for their input on further measures they would like to see in an internet voting system (e.g. "In your opinion what other information should be available about the internet voting system"). At the end of the TDIV questionnaire the participants were furthermore asked an open-ended question about further measures that they believe would increase transparency in an internet voting system. The questionnaire concluded with questions about participants' trust in authorities.

5 Items retained for the survey are available at https://github.com/comet-itu/constructs/blob/main/Codes_constructs.pdf

6 https://www.soscisurvey.de, last accessed 03.02.2023.

7 https://www.prolific.co/, last accessed 03.02.2023

Data Analysis: We examined the data after collecting it from the participants for missing values, questionable response patterns, and data distribution, as common when collecting quantitative data from participants (Hair et al. 2021a). Furthermore, we tested for outliers and straight-line response patterns, and these types of responses were rejected and removed if they also failed the attention checks questions.

For the analysis, the data was analysed using the IBM SPSS statistical program and Partial Least Square Structured Equation Modeling (PLS-SEM) with the SmartPLS software package (Ringle et al. 2022). We chose this second-generation statistical method (PLS-SEM) over others, such as factor or regression analysis, because PLS-SEM is suitable for multivariate analysis; it has the capacity to manage and test for complex relationships between independent and dependent variables (Hair et al. 2021a; Hair et al. 2021). Note that even though PLS-SEM is a non-parametric statistical method, it is critical to ensure that the data is not out of normal range, as this can cause mistakes in the results (Hair et al. 2021a). As a result, we investigated the various measures of distribution, mean and standard deviation (which estimates the amount of data scattered around the mean).

Ethics: Our institution does not require ethical approval for conducting a user study; however, we followed the APA ethical guidelines (Americal Psychological Association 2017) for conducting both a pilot study and a survey. Before initiating the process, we informed the participants about our study's goals and explained that they could withdraw from the study at any time. According to the privacy and confidentiality section of the APA guideline (Americal Psychological Association 2017), the participants were informed and assured that their responses would remain confidential and only be used for research purposes. These responses would be used by the researchers involved in the study in an anonymous form during publication. In addition, we also notified our participants before starting the study that attention checks are present and failing them will lead to no compensation from the Prolific platform. We furthermore provided our contact details to participants in case of further questions or concerns.

4. Results

This section presents the findings of the study. We followed a two-step analysis approach, as in PLS-SEM, by evaluating the reflective measurement model and the structural model (Hair et al. 2021a; Hair et al. 2021b). In evaluating the reflective measurement model, we assess the model's quality by measuring the relationship between the indicators and the dimensions as well as the relationship between dimensions. Furthermore, we assess the indicator's reliability, internal consistency reliability, convergent validity, and discriminant validity. After assessing the quality of the measurement model, we evaluate the structural model by examining the collinearity issues in the model, the path coefficient of the structural model, and the model explanatory power. Note that a total of 514 participants have been recruited in the study, of which 14 were excluded based on low-quality responses, such as failed attention checks (see Table 1 and Appendix A in the appendix). Out of the remaining 500, 245 identified as women, 252 as men and three as non-binary. More than half of the participants (281) were between ages 18 and 40. The full participant demographics are provided in Table 1 in the appendix.

4.1. Analysis of the reflective measurement model

To test the reflective measurement model, we first examined its reliability by looking at the indicators' outer loading. The rule of thumb is that the outer loading should be 0.708 or higher (Hair et al. 2021a), and practically all indicators' outer loading surpasses the threshold. However, there were a few indicators that were lower than the acceptable 0.708 but greater than 0.4; for example, InfAv07 = 0.665, RemMs02 = 0.614, and Test04 = 0.657. These indicators were kept because their removal did not affect the reliability or validity of our model (Hair et al. 2021a). Nevertheless, we removed InfAv03 = 0.619 and RemMs06 = 0.519 because these indicators affected our "Average Variance Expected" (AVE). Furthermore, we examined our model's internal consistency reliability by using Cronbach's alpha and composite reliability. However, due to Cronbach's alpha (Hair et al. 2021a) limitations, we used composite reliability (CR) to assess the internal consistency reliability. Our results, refer to Table 2 in Appendix A, reveal that the CR values were within the acceptable range, namely between 0.60 and 0.90 (Hair et al. 2021a), confirming the model's internal consistency reliability. In addition, we assessed the convergent validity of the identified dimensions. Our results, refer to Table 2 in the appendix, reveal that the AVE of all the latent variables or the dimensions were above 0.50. This demonstrates that, on average, all latent variables may account for more than half (50 per cent) of the variance of their indicators (Hair et al. 2021a). Further, we evaluated the discriminant validity. Thereby, we adopted the Heterotrait-Monotrait ratio (HTMT), which has been suggested to be a more trustworthy measure to determine discriminant validity (Hair et al. 2021a; Hair et al. 2021b). Our findings show that the values were below the acceptable threshold level, namely 0.85, indicating that the identified dimensions are conceptually distinct.

4.2. Analysis of the structural model

For the structural analysis, we followed the method suggested by Hair et al. (2021a, 2021b). First, we examined both the outer and inner models for collinearity issues. Our findings show that collinearity was not an issue for our model. All the values were below the threshold of 5. Hence, there was no collinearity among the dimensions. Further, we examined the significance of the relationships between the structural model. The results, refer to Table 3 in the appendix, showed that information availability ($\beta = 0.175$, $p = 0.003$), monitoring and verifiability ($\beta = 0.217$, $p = 0.000$), remedial measures ($\beta = 0.225$, $p = 0.001$), and testing ($\beta = 0.217$, $p = 0.000$) have a positive correlation with transparency. Thus, providing support for the hypotheses H1, H3, H4 and H5. However, there was no correlation between understandability ($\beta = -0.018$, $p = 0.746$) and transparency. Hence, hypothesis H2 was not supported. From the findings, shown in Table 4 in the appendix), it can be inferred that remedial measures (0.225) have the strongest correlation with transparency, followed by testing, monitoring and verifiability (0.217). In contrast, information availability (0.175) has only a minor correlation. Finally, we investigated our model's explanatory and predictive power. We looked at the coefficient of determination (R2) of our endogenous dimension (transparency) to test its explanatory power. We found out that our model had 40% explanatory power for transparency, with an R2 of 0.407. This indicates that our model has moderate explanatory power (Hair et al. 2021b). To evaluate our model's predictive power, in particular, to assess whether our model can be generalisable and make future predictions using different data sets, we used the "PLSpredict" procedure

proposed by Hair et al. (2021a, 2021b). Thereby, we assessed the dependent variable "transparency" and its root mean square error (RMSE), as well as Q2 prediction. This means that we compared the values generated by PLS-SEM RSME against the values produced by the linear regression model (LM) benchmark. The results from our analysis show that all values for the "transparency" indicators in the PLS-SEM RMSE (Trans01, Trans02, Trans03, Trans04) are lower than the values for LM RSME. Consequently, our model has a high predictive power. The Q2 predict values for the indicators (Trans01, Trans02, Trans03, Trans04) are all greater than zero, confirming that our path model performed better than the LM benchmark.

4.3. Qualitative analysis

In this section, we report the results of the open-ended questions where we asked respondents about the additional measures which could be taken into consideration for each of the five individual studied dimensions as well as transparency in general. The goal of the analysis was to gain further insights into which measures related to each dimension as well as transparency measures outside of the identified dimensions.

The responses were analysed by three of the authors using thematic analysis. For analysing the open-ended questions related to the five dimensions, we followed an inductive approach. We looked at each open-ended question related to five dimensions individually and gathered the responses in codes8. These codes were combined under different themes in each dimension. We used this approach as it gave us insight into the transparency measures for each dimension, which we had not discussed in our questionnaire. For example, when asked about what other information should be available about the internet voting system, we noticed in our analysis that the participants mentioned they would like to have information about their personal and voting data. This measure was not originally included in our dimension, but from the analysis, it came out as a key transparency measure for the "information availability" dimension. Note, while our questionnaire asked questions specifically related to each individual dimension (e.g. "In your opinion, what other information should be available about the internet voting system?"), upon analysis, we noticed that the responses did not always follow this distinction, e.g. with participants mentioning the need for verification methods when asked about information that should be available about the system. We used a deductive approach with the open-ended question related to general transparency (e.g. "In your opinion, what kind of measures should be taken to increase the transparency in the internet voting system?") where we already had these five dimensions and a set of themes with codes. We looked at responses from the participants and either coded them as related to one of these dimensions or treated them as a separate theme related to transparency. For each one of the individual questions, codes that had less than ten responses (2% of respondents) and could not be merged with the rest of the codes were omitted from the rest of the analysis.

8 Note that we did not code answers that were not clear or did not relate to the question that was asked

4.3.1. Information availability

When answering questions about what other information should be available about the internet voting system, we classified the participants' responses into the themes: *personal data protection, security of the votes, system workings, voting process, election results, verification methods*, and *audits*.

Personal data protection: The participants expressed the need to have information about how their personal and voting data would be handled. As such, the participants asked the following questions: who can view my data, how long will the data stay in the system, when is it going to be deleted, how the data is going to be used, including potential threats to the secrecy of their vote *("How many people (of the company running it) can access the information. Can anyone link up the vote to the person who cast it?")*. Information around data security was important for the participants as they wanted to protect their information from unauthorised access, use, and disclosure. As such, the participants want to protect their data from disruption, modification, or destruction. They expect to have clear information on security measures taken when their data is transferred and stored *("I would like to see detailed information on security measures to combat voter fraud. Specifically, in cases such as multiple votes being cast, identity theft or people who don't normally vote having their information used without their knowledge to cast votes")*. Also, in case of a security breach, the participants want to know what information has been compromised *("Information on what data has been extracted and whether that comprises of a personal data breach")*. The participants emphasised a full disclosure by an independent auditor and a summary of the effect on the outcome.

Security of the votes: The participants mentioned the need to have information about the security of the internet voting system and the security measures taken to prevent the violation of election *integrity ("I think people need to know who and how ensures that the system is safe, will not be hacked, etc.")*. They expressed concern about the security of the online voting system by asking questions such as *"how secure the voting system is, i.e. is it easy to hack?"* or *"where the votes go, what the security protocol is, what happens if they're hacked?"*. Even though participants pointed at the security of the voting system, they proposed specific security measures such as voter authentication and stringent fraud checks to *"ensure there are no attacks or interventions"*. Also, they mentioned that the voting system should provide an assurance against vote manipulation to benefit a specific party *("I would need to feel confident it isn't open to abuse/ vote rigging")*.

System workings: The participants indicated that the information about the working of the internet voting system should be disclosed to the public, and they specifically wanted to know how the information, such as handling and processing of the vote, is executed, which entities are involved in implementing it, are these entities audited by an independent organisation *("How it works, who is allowed to vote, how votes will be handled, which individuals will be processing the votes, how will those individuals be audited")*. The participants also asked for the disclosure of information about vendors or companies involved in developing and implementing the internet voting system *("The vendors of the system should definitely be known to the public")*. There was a clear emphasis on a thorough background check of the company and its employees who had developed the system. The participants also wanted to know whether the vendor had any history of compliance issues or had any political affiliations *("Does the vendor have any incidence of data loss in their background, and do a majority of their*

major shareholders donate to any political party?"). The participants were of the view that if such information is made available to the public, it will increase transparency, and the vendors could be held accountable if there are any election irregularities *("Any company/organisation involved should be clearly and freely identified. Full transparency means that they are able to be held to account and reduce fraud/election rigging")*.

Voting process: The participants mentioned the need for detailed information on how to execute the online voting process *("Plenty of information about how to vote online and a step by step guide")*. Such step-by-step instructions on registering the vote reduce the voters' effort and increases their confidence in the voting process. It also gives them a clear view of*"where to vote, how to vote and the options of voting as well as the deadline"* associated with the voting process.

Election results: The participants emphasised the detailed information on how the votes are counted and the results generated *("Details on how the internet votes are dealt with and counted")*. The participants mentioned that they would prefer the involvement of independent experts during the vote counting and certification of election results to maintain electoral integrity.

Verification process: Participants also expressed an interest in learning more about the internet voting verification process. That is, they want to know how voters are verified to vote *("How they can verify who you are"),* and how votes/ballots are recorded *("is there any way i can double check that my vote was recorded the way I wanted it to be after the results are given?")*, and finally, if their votes are counted as recorded *("A way to check your vote has been counted", "A way for a person to confirm that his/her vote was correctly counted")*

Audits: Finally, regarding audit information, participants mentioned the importance of making all audit reports publicly available to all citizens so that anyone can obtain an audit of the election process *("If the audit reports were freely available to the public ", "Publication of external audit reports"*).

4.3.2. Understandability

When answering questions about what other aspect of the internet voting system you would like to understand, we classified the participants' responses into the following sub-themes: *understanding security measures, how the voting system works, verification process, accessibility and support* and *data storage*.

Understanding security measures: Participants expressed the need to understand the security measures employed to ensure that the vote cast is secured *("What security measures the internet voting system takes to ensure no foul play.", "how the votes are made secure, given the sophistication of hackers")* as well as how to prevent the vote cast from being tampered with *("I would also need to know how votes could be prevented from being tampered with").* Other participants mentioned the need also to understand how the system could be protected from outside attacks, such as hacking *("Security against possible hacking")*.

How the voting system works: Regarding how the voting system works, participants mentioned the need to understand the various aspects of the voting system, such as how to cast their votes *("How*

to cast a vote,", "The process of voting"), an explanation of the voting procedure *("I'd want to see a visual flow chart explaining what happens within the system at every step", "Step by step guide on how to vote electronically"),* as well as how the votes are counted *("I would like to understand the process of how votes are counted when an internet voting system is used").*

Verification process: Participants mentioned the need to understand the verification process when they cast their votes *("How verification occurs to stop fraud", "how they are verified")* as well as how the final votes are counted and verified *("The proof that the votes are counted correctly.", "The proof that the votes are counted correctly.")*. Furthermore, some of the participants also mentioned the need to understand how voters are authenticated before casting their votes *("ID checks to make sure each person only votes once", "There should be some control over the identity of the person that is voting. Sometimes the children of old people vote instead of them", "How they ensure a voter is genuine, exists, is eligible").*

Accessibility and support: Participants expressed the need to make the voting system more understandable to the elderly as well as people without technical backgrounds *("easy to understand for old people.", "Elderly or people with not much technical experience should be able to use a representative")*. Furthermore, some participants also expressed the need to provide help and support to those who may struggle to use the voting system *("Support for people who struggle at voting hubs", "How to support others to use the voting system ")*.

Data storage: Finally, with regards to data storage, participants mentioned the need to understand how their data will be collected, processed, and stored *("How all the data is stored and collected", "How is sensitive data handled")*. The participants further mentioned the need also to understand how long their data is stored ("*How the information is stored and for how long*") as well also who has access to this data *("I would like to know where the data is stored, who is accountable for the data")*.

4.3.3. Monitoring and verifiability

When answering the question "What would increase your confidence that the result of the verification is accurate?" the participants mentioned the themes of *openness of verification, individual verifiability, results, verifier characteristics, limitations of verification, security* and *general monitoring*.

Openness of process: Participants expressed the need for the verification processes to be open and transparent, as well as clearly communicated to the *public ("Open and honest communication in regards to process and results")*. Some mentioned their wish to see information about the process itself *("Processes being released to the public")*, entities involved in the verification *("Transparency around the companies and processes involved in checking the results")*, as well as documentation about the voting system *("Detailed reports and technical reports of the system used.")*. Others furthermore suggested involving media in publicising the tallying process, e.g. via public broadcasting *("Proof of actual video report of counting votes as they are being counted")*.

Individual verifiability: Participants mentioned the need for the voters to be able to verify the correctness of their vote *("Being able to see and verify my vote")*. Some furthermore expressed the wish to receive a receipt of their vote as a confirmation, delivered, e.g. by email *("A notification email to show that my vote had been registered with the party of choice")*. At the same time, participants expressed the

importance of reconciling such individual verification with vote secrecy *("It would be good to be able to see what you have voted but for the vote not to be available for others to see and identify who voted for who")*.

Results: Participants mentioned relying on the published election results as a means to detect election integrity violations. As such, participants noted that results being within their expectations would increase their confidence in elections *("the result is one I would reasonably expect")* or asked for a detailed reporting of the results *("Openness on the results within each area")*.

Verifier characteristics: Participants mentioned characteristics they would like to see in parties or entities performing the verification. As such, some stressed the importance of such entities in being independent and not affiliated with any of the political parties *("An independent authority checking internet cast votes who are not connected with the political spectrum")* or having representatives from multiple parties performing the verification *("Multiple people from different political parties have verified the process is accurate.")*. Other responses focused on the expertise of the verifiers in conducting the verification *("Seeing expert opinions from individuals and companies who know what they are talking about that say they have found no irregularities")*.

Security: Participants mentioned the need for strong security measures to prevent election integrity violations. Some mentioned specific measures, such as strong authentication *("A two-layer process to verify it's me voting (as in online banking for example) or fingerprint recognition.")*, while others emphasised the importance of ensuring security in general *("If the securty involved could be guaranteed to keep potential tampering, data breaches or accidental loss equal or lower in number to a paper ballot.")*.

4.3.4. Remedial measures

When answering questions about what other remedial measures participants would like to see about the internet voting system, we classified the participants' responses into the following subthemes: *notification about breaches, assurances about the security of votes/personal data, openness, support for the voters, accountability*, and *re-voting*.

Notification about breaches: Several participants mentioned the need to provide timely notifications about any security breaches within the voting system, particularly notifying the affected voters *("To know ASAP and to what effect has been breached")*. Further, some participants mentioned the need to notify the voters about the extent to which their personal data has been breached and possible consequences, e.g. as risks for identity fraud *("A voter should be warned and explicitly told that data may have been breached")*.

Openness and accountability: People furthermore mentioned the need for explanations about the breach, its causes and how it is handled *("Explanation of why and how and how this will be prevented further")*, as well as the importance of transparent processes on how the breach is being handled, including involvement of independent parties and comprehensive reporting about steps being taken *("A report from an independent body explaining the breach, what has been done to rectify it with the correct votes being tallied, and efforts are being made to identify the party responsible to pass over to law enforce-*

ment"). Other participants mentioned the need to hold the parties responsible for the breach accountable *("Public accountability for the data breaches")*, as well as the need for legal persecution *("clear laws that prosecute those who allow fraud either deliberately or through negligence.")*.

Assurances about the security of votes/personal data: The participants mentioned the need to be reassured that the consequences of the breach have been safely handled *("They need to know the issue is being dealt with")*. In particular, some mentioned the need for reassurances that their personal data is safe *("Reassurance their personal details are not compromised")* or that their vote has been counted correctly ("Assurance that his/her/their vote has still been counted correctly").

Support for the voters: The participants also mentioned the need to provide different kinds of support to the voters, such as an easy way for the voters to report breaches or any kind of suspicious activity within the voting system *("An easy way to report any suspicions")*. Others also mentioned a need for easily accessible contact information for getting support, i.e. as a phone number or email *("A chat line on the system or a telephone helpline (fully manned during the election process in order to avoid long waiting times)")*. Furthermore, participants also mentioned the need to get actionable instructions to ensure that their vote is counted *("what steps they need to take to submit their vote correctly.")* and/or that their personal data is secure *("Clear information and actionable steps they can take to protect their personal data")*.

Re-voting: Finally, participants also mentioned the need to request the voters to recast their votes *("that they can submit the vote again")*, or in most critical cases, to repeat the election in case of any breach *("Elections should be stopped and restart all over again")*. Some participants furthermore mentioned the necessity of providing alternative voting channels to avoid using the internet voting system in case of issues *("The ability to recast their vote using another method")*.

4.3.5. Testing

When answering the question about testing measures within the system they would like to see, the participants' responses were classified into the following sub-themes: *general testing, technical testing, user testing, trial voting, tester characteristics and testing communication*.

General testing: Participants commented on the general need to test the system before the election without mentioning details on how such testing should be conducted. As such, the participants stressed the need to test every step of the election *("the whole system from advertising to result count issue.")* and the expected thoughtfulness of such testing *("It should be throughly tested for months and months before being used for something very important")*.

Technical testing: A number of participants mentioned the need to test the technical quality of the system. As such, participants suggested to conduct stress testing *("All software has bugs, despite testing and expert review. Stress testing will be important.")*, test the system for its ability to handle a large number of voters *("that the system can handle thousands of people logging into vote at once.")* and its security *("Test all potential security holes in the system. Don't try to save money from not doing everything thats possible to test.")*. Additionally, the participant recommended penetration testing *("Pen testing*

by a variety of sources ", "They should take attempts to hack it to see how strong their security is") as well as testing security breaches *("System tested against hacking and breaches of privacy", "Seeing if any security breaches happened in the test.")*.

User testing: Participants mentioned the importance of ensuring that the system is easy to use by the voters *("That it is simple enough for everyone to use")*. They furthermore noted the need to test the systems for their accessibility for disabled voters *("accessibility testing to ensure it is usable for people with different disabilities and with different accessible technologies")* and suggested testing the system involving voters from different socio-demographic groups *("have it tested by a sample of people from different age groups to determine the ease of use of the UI")*.

Trial voting: Before the election, participants suggested organising ways to test the system in trial runs, either conducting mock elections *("a dry run with fictional parties")*, using the system in low-stake elections *("Use it for real in less important ballots several times.")* or making it available only to a small group of voters first *("Running a trial in a certain area first to ensure it works as it should once all the testing has taken place.")*. Some responses furthermore suggested using the test trials to compare the resulting tally with the tallied votes collected by another channel, e.g. paper ballots *("A limited number of potential voters should test the system with their answers also being submitted on paper to ensure the correct information is stored on the voting system")*. Participants furthermore suggested providing an option to test the system to individual voters before casting their actual vote *("I think you should be able to try out internet voting beforehand, so we can prevent those problems where people vote for the wrong thing.")*.

Tester characteristics: A number of responses focused on involving people with specific characteristics as testers. As such, participants mentioned the importance of involving experts, including security experts or ethical hackers, in testing the system *("Security experts must test the system thoroughly and identify any problems.")*. Further responses stressed the importance of testers being independent of political affiliations *("Independent testers with no affiliation to any party or anything to gain")* or involving testers from multiple political parties to reduce biases in the testing outcome *("Each party should be allowed to put a self selected expert forward to audit the software and all parties must agree that they are happy with how the software works.")*. Participants furthermore noted the importance of involving the general public in the testing *("Everyone who is going to use should be asked to test, not just a small proportion of the public")*; however, a few responses mentioned that such an involvement would be unnecessary or even confusing *("it should be tested extensively, but not public to avoid confusion")*.

Testing communication: Participants mentioned the importance of communicating information about the system as well as informing them about the testing processes. As such, responses mentioned providing information about using the system via various media channels such as television or the internet *("Information and tutorials should be made publically available and possibly even widely disseminated via many different platforms.")*. Others mentioned the need to disseminate testing results to the public *("there should be a lot of testing and results to show the public to make sure they understand how secure it is")*.

4.3.6. General transparency

When answering the question, "What kind of measures could be taken to increase the general transparency of the internet voting system?" The responses addressed the themes already present in the five dimensions as described above. For the sake of brevity and to avoid repetition, we therefore omit the detailed description of themes related to the five dimensions, as they are described above

4.3.7. Further findings

While our analysis focused on identifying transparency-enhancing measures, a number of responses suggested other overarching themes that shed light on the perception of transparency in internet voting. As such, several respondents expressed scepticism towards being able to achieve transparency *("I don't think it can be fully transparent")*, as well as expressing doubts about whether it is possible to verify the election integrity *("Not sure. Any verification could be inaccurate")*. Other participants furthermore had concerns about potential vote secrecy issues resulting from verification *("I would be a little concerned about Election authorities monitoring throughout..could the vote be traced back directly to me. ")*, or interpreted transparency as a potential risk, believing that revealing too much information about the system would make it easier for malicious actors to compromise it *("The problem is that the level of transparency required would enable hackers more insight in to how to manipulate.")*.

5. Related work

A number of studies investigating the role of trust in e-voting and related factors (such as perceptions of risks and benefits), as well as factors affecting such trust, have been conducted (Sindermann et al. 2023; Kapsa and Musial-Karg 2022, 12; Vassil et al. 2016; Duenas-Cid 2022). As such, Duenas-Cid investigates the questions of trust and distrust in electronic voting in a number of works (Duenas-Cid 2022; Duenas-Cid 2024), arguing that these concepts are distinct from each other (i.e. distrust is not simply a lack of trust) and that transparency plays a role for both of them (Duenas-Cid 2022). Licht et al. (2021) furthermore identified trust as as one of the main driving factors in the adoption of internet voting. A systematic literature review of factors affecting trust (Erb et al. 2023) identifies transparency of the voting process, defined as a voter's ability to observe every step of the election process, as one of these factors. Other identified factors include the understandability of the election process, the presence of the verification mechanism, the presence of other security-related mechanisms (e.g. authentication), and overall perception of the system's security, for instance, based on knowledge about data breaches, conducted audits, or available explanations provided by experts. These factors align with our findings, covering the transparency dimensions of information availability, understandability, verifiability and testing of TDIV.

Further works analyse case studies of existing elections, such as using voting machines in the Netherlands (Duenas-Cid 2024), internet voting in elections in Ontario (Goodman et al. 2023) and attempts to introduce internet voting in Åland Islands. These case studies, in particular, outline is-

sues related to the dimensions investigated in our study, such as lack of oversight and vendor transparency, televised demonstrations of system vulnerabilities by activist groups, insufficient government response, challenges with integrating verifiability into existing electoral procedures, and technical and legislation issues resulting in delays of auditing processes. The findings, therefore, confirm the importance of all five TDIV dimensions.

6. Discussion and conclusion

Our findings revealed several groups of measures (dimensions) that are important to voters in terms of internet voting transparency. The findings from our study showed that participants' attitudes towards information availability, monitoring and verifiability, remedial measures, and testing are strongly correlated with their perceived importance of transparency, suggesting that proper implementation of these measures is of significant importance for ensuring that the voters perceive an internet voting system as transparent.

Information availability: The findings demonstrated the significance of making documentation about the internet voting system publicly available. Such documentation should demonstrate how the internet voting system functions, as well as the underlying security mechanism(s). Voters also want public information about the vendor(s) who supplied or developed the internet voting system, allowing them to determine whether the acquisition or implementation of the internet voting system was not influenced by the government or political parties. As providing such information aligns with common recommendations by election experts (Buckland et al. 2011), our findings confirm its importance. Our qualitative analysis has furthermore shown that voters are interested in learning more about data protection policies of the voting system, which are not limited to protecting the secrecy of the vote – which points to increased awareness about such issues following the introduction of the GDPR and other data protection legislation.

Monitoring and verification: Our findings also revealed that individual and universal verifiability, as well as other measures implemented to monitor the integrity of election processes, are linked to voters' positive attitudes toward the transparency of the internet voting system. Furthermore, this finding is reaffirmed by our qualitative analysis, with participants mentioning the need for both universal verification by third parties, such as trusted experts and individual verification by voters themselves. The argument that implementing verifiability measures is necessary for voters' trust and perceived transparency has been put forward by previous research (Agbesi et al. 2022; Marky et al. 2022), as well as supported by other previous studies in the context of Estonian elections (Solvak 2020). It is worth noting, however, that the attitudes towards verifiability can be paradoxical. Some studies show that voters do not understand the purpose of verifiability and do not see the need to conduct the verification themselves (Olembo et al. 2014). Furthermore, empirical data from real-world elections show low voter verification rates (e.g. around 5% in Estonian elections (Ehin et al. 2022)). It can, therefore, be argued that while the presence of verifiability options can and does serve as an assurance to the voters, more work needs to be done to ensure that it is understood and utilised to its full extent.

Remedial measures: In terms of remedial measures, the findings suggest that stakeholders should not only make an effort to implement measures to detect and prevent any security breaches that may occur during the voting process but also make sure that the existence of such measures and the extent to which independent experts have audited them is adequately communicated to the voters.

In particular, our qualitative analysis stresses the importance of having available reporting channels through different modalities (e.g. email, phone, or online form). The existence of such channels should be clearly communicated to all the voters, and feedback should be provided to the voters who report irregularities with the election, including support in case any actions are required from the voter (e.g. instructions on how to revote in case there are issues with the voter's initially cast vote).

Our findings furthermore stress the importance of providing clear notifications of the security issues, especially to voters directly affected by the breach. The notification should include an overview of how exactly the individual voters or the election, in general, is affected (e.g. which personal data has leaked), which risks can result from the breach (e.g. risks of identity theft due to leaked personal data of voters) and which actions should the voters take to minimise these risks.

Another important aspect is informing the voters about how the breach is handled. This includes reassuring them that their data is safe and that their vote will be counted (providing this is the actual truth), as well as informing them on which steps are taken to minimise the impact of the breach as well as to prevent further breaches in the future. Transparently handling the breach furthermore includes ensuring accountability by explaining to the voter why the breach has happened and how responsible parties are being handled. In particular, if malicious intent is evident, voters must be reassured that the responsible parties face appropriate consequences. e.g. in the form of legal persecution.

Even though studies (Saldanha and Silva 2020) have found that measures such as accountability do not influence voters' attitudes toward transparency, our findings showed otherwise.

Testing: Our study also provided sufficient evidence that testing the internet voting system by experts and the general public prior to its use significantly impacts voters' attitudes towards the system's transparency. Such an approach, in particular, has been used for the Swiss voting system, which provided opportunities for public testing, including election security experts. While the testing revealed a number of serious vulnerabilities, preventing its use in the election, its contribution to the transparency of internet voting elections was commented positively by experts (Driza Maurer 2019). Our study showed that this is likely to be positively perceived by the voters as well. In particular, the findings of our study stress the importance of conducting trial runs and mock elections, as well as introducing the system gradually by using it in smaller-scale elections first. The qualitative results of our study furthermore emphasised the need to involve voters in the testing process, including voters from diverse demographics, and involve independent experts in conducting the testing.

Understandability: There was insufficient evidence from our quantitative analysis to support that understandability correlates with voters' attitudes toward internet voting transparency. One possible explanation is that while understanding the internet voting system may be important to voters (e.g. improving their self-efficacy in using the system to vote), it is not necessarily perceived as contributing to transparency. Indeed, previous research shows that voters' understanding of an internet voting system does not necessarily contribute to voters' trust in the system and might even have a negative impact (Zollinger et al. 2021). Nonetheless, a number of suggestions have been made by our participants in the qualitative part of the study, with participants expressing the need to understand the security features of the system, its verification processes as well as its data protection policies, suggesting that presenting this information in an accessible way indeed has a potential of positively influencing voters' trust in the voting system. Thus, a relationship between understandability, transparency and trust might have a paradoxical nature in that voters believe that they need to understand how the system works to see it as transparent and/or trustworthy. Still, their actual reactions to being provided with explanations demonstrate a different effect. Therefore, further investigations regarding this understandability paradox, which might have similar explanations as the so-called privacy paradox (Kokolakis 2017), are needed.

Finally, while the proposed measures can potentially improve the transparency of the voting system and reduce security risks, they have their limitations that need to be acknowledged, such as verifiability techniques often being difficult for the voters to apply (Volkamer et al. 2022) or difficulties in addressing threats such as voter coercion. Therefore, the decision on whether to provide the option to vote online should therefore be made on a case-to-case basis by experts from both technical and social disciplines, and in case such an option is provided, additional channels (e.g. traditional voting in polling places) should be offered to voters who either prefer not to vote online or experience issues with the voting process (as done e.g. in Estonian elections (Ehin et al. 2022)).

Limitations: Even though the findings highlighted several important aspects of transparency, the survey has some limitations that must be considered. First, as only a few countries implement internet voting on a large scale, most of our participants did not have personal experience with internet voting systems. While their experiences still provide valuable insights for introducing internet voting in countries without such prior experience, the extent to which our findings would differ in countries with an extensive history of internet voting, such as Estonia, remains to be studied. Furthermore, while our literature review was conducted systematically, it is not exhaustive. We did not include technical papers, such as the work by Küsters and Müller (2017) and Bernhard et al. (2017), and did not include research findings from other domains within information technology, such as machine learning (ML) and decision support systems (Schmidt et al. 2020; Kizilcec 2016, Branley-Bell, D., Whitworth, R., Coventry 2020), automation systems (Lyons et al. 2017; Yang et al. 2017), social media algorithms (Rader et al. 2018) and automatic online comment moderation systems (Brunk et al. 2019). A more comprehensive and thorough examination of relevant literature could provide deeper insights and enhance our understanding of the relationship between transparency and trust in internet voting, consequently influencing the definition of transparency and its dimensions.

Future work: Our study focused on correlations between voters' perceived importance of various types of measures commonly treated as transparency- related by researchers and practitioners when applied to internet voting- and the perceived importance of transparency in general. To further validate our findings, a thorough and comprehensive literature review, along with additional research—such as controlled experiments—is necessary to understand whether the presence of these measures in a voting system has a significant effect on the perceived transparency of the system, as well as on trust and willingness to use the system for real-world elections. A particularly interesting research direction would be to investigate the effects of understandability further. As our study showed mixed results, the extent to which understandability influences perceived transparency and trust, as well as the appropriate ways to provide understandability (e.g. determining the contents as well as the media for providing voters with explanations about the system).

References

Acemyan, C.Z., Kortum, P., Oswald, F.L.: The trust in voting systems (tvs) measure. International Journal of Technology and Human Interaction (IJTHI) 18(1), 1–23 (2022)

Agbesi, S., Dalela, A., Budurushi, J., Kulyk, O.: "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. E-Vote-ID 2022 p. 1 (2022)

Aithal, A., Aithal, P.: Development and validation of survey questionnaire & experimental data–a systematical review-based statistical approach. International Journal of Management, Technology, and Social Sciences (IJMTS) 5(2), 233–251 (2020)

Association, A.P., et al.: Apa. ethical principles of psychologists and code of conduct; 2017

Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y.A., Stark, P.B., Teague, V., Vora, P.L., Wallach, D.S.: Public evidence from secret ballots (2017), https://arxiv.org/abs/1707.08619

Branley-Bell, D., Whitworth, R., Coventry, L.: User trust and understanding of explainable ai: exploring algorithm visualisations and user biases. In: International Conference on Human-Computer Interaction. pp. 382–399. Springer (2020)

Brunk, J., Mattern, J., Riehle, D.M.: Effect of transparency and trust on acceptance of automatic online comment moderation systems. In: 2019 IEEE 21st Conference on Business Informatics (CBI). vol. 1, pp. 429–435. IEEE (2019)

Buckland, R., Teague, V., Wen, R.: Towards best practice for e-election systems. In: International Conference on E-Voting and Identity. pp. 224–241. Springer (2011)

Cid, D.D.: A theoretical framework for understanding trust and distrust in internet voting (2022)

Driza Maurer, A.: The swiss post/scytl transparency exercise and its possible impact on internet voting regulation. In: International Joint Conference on Electronic Voting. pp. 83–99. Springer (2019)

Duenas-Cid, D.: Trust and distrust in electoral technologies: what can we learn from the failure of electronic voting in the netherlands (2006/07). In: Proceedings of the 25th Annual International Conference on Digital Government Research. pp. 669–677 (2024)

Ehin, P., Solvak, M., Willemson, J., Vinkel, P. Internet voting in estonia 2005–2019: Evidence from eleven elections. Government Information Quarterly 39(4), 101718 (2022)

Erb, Y., Duenas-Cid, D., Volkamer, M.: Identifying factors studied for voter trust in e-voting – review of literature. Proceedings of 8th International Joint Conference on Electronic Voting (E-Vote-ID 2023) (2023)

Faraon, M., Stenberg, G., Budurushi, J., Kaipainen, M.: Positive but skeptical : A study of attitudes towards internet voting in sweden. In: CeDEM Asia 2014 : Proceedings of the International Conference for E-Democracy and Open Government. pp. 191–205 (2015)

Federal Constitutional Court of Germany: Decisions: Order of 03 March 2009- 2 BvC 3/07 (2009), http://www.bundesverfassungsgericht.de/SharedDocs/ Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html, last accessed August, 20, 2024.

Fragni`ere, E., Gr`ezes, S., Ramseyer, R.: How do the swiss perceive electronic voting? social insights from an exploratory qualitative research. In: International Joint Conference on Electronic Voting. pp. 100–115. Springer (2019)

Goodman, N., Spycher-Krivonosova, I., Essex, A., Brunet, J.: Verifiability experiences in ontario's 2022 online elections. In: International Joint Conference on Electronic Voting. pp. 87–105. Springer Nature Switzerland Cham (2023)

Hair, J., Hult, G., Ringle, C., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publications (2021), https://books.google.dk/books?id=6z83EAAAQBAJ

Hair Jr, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Danks, N.P., Ray, S.: Partial least squares structural equation modeling (pls-sem) using r: A workbook (2021)

Hall, J.L.: Transparency and access to source code in e-voting. In: USENIX/ACCURATE Electronic Voting Technology Workshop (2006)

Jain, S.S., Jain, S.P.: Power distance belief and preference for transparency. Journal of Business Research 89, 135–142 (2018)

Kapsa, I., Musial -Karg, M.: Risks and benefits of i-voting in public opinion: Evidence from poland. Polish Political Science Yearbook (1 (51), 163–180 (2022)

Kizilcec, R.F.: How much information? effects of transparency on trust in an algorithmic interface. In: Proceedings of the 2016 CHI conference on human factors in computing systems. pp. 2390–2395 (2016)

Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security 64, 122–134 (2017)

Ku¨sters, R., Mu¨ller, J.: Cryptographic security analysis of e-voting systems: Achievements, misconceptions, and limitations. In: Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schu¨rmann, C. (eds.) Electronic Voting. pp. 21–41. Springer International Publishing, Cham (2017)

Licht, N., Duenas-Cid, D., Krivonosova, I., Krimmer, R.: To i-vote or not to i-vote: Drivers and barriers to the implementation of internet voting. In: Electronic Voting:

6th International Joint Conference, E-Vote-ID 2021, Virtual Event, October 5–8, 2021, Proceedings 6. pp. 91–105. Springer (2021)

Lyons, J.B., Sadler, G.G., Koltai, K., Battiste, H., Ho, N.T., Hoffmann, L.C., Smith, D., Johnson, W., Shively, R.: Shaping trust through transparent design: theoretical and experimental guidelines. In: Advances in human factors in robots and unmanned systems, pp. 127–136. Springer (2017)

Marky, K., Gerber, P., Gu¨nther, S., Khamis, M., Fries, M., Mu¨hlha¨user, M.: Investigating {State-of-the-Art} practices for fostering subjective trust in online voting through interviews. In: 31st USENIX Security Symposium (USENIX Security 22). pp. 4059–4076 (2022)

Marky, K., Zollinger, M.L., Roenne, P., Ryan, P.Y., Grube, T., Kunze, K.: Investigating usability and user experience of individually verifiable internet voting schemes. ACM Transactions on Computer-Human Interaction (TOCHI) 28(5), 1–36 (2021)

Nurse, J.R., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., Goldsmith, M., Creese, S.: An assessment of the security and transparency procedural components of the estonian internet voting system. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 366–383. Springer (2017)

Olembo, M.M., Renaud, K., Bartsch, S., Volkamer, M.: Voter, what message will motivate you to verify your vote? In: Workshop on Usable Security (2014)

Oppenheimer, D.M., Meyvis, T., Davidenko, N.: Instructional manipulation checks: Detecting satisficing to increase statistical power. Journal of experimental social psychology 45(4), 867–872 (2009)

Portes, A., N'goala, G., Cases, A.S.: Digital transparency: Dimensions, antecedents and consequences on the quality of customer relationships. Recherche et Applications en Marketing (English Edition) 35(4), 72–98 (2020)

Puiggali, J., Cucurull, J., Guasch, S., Krimmer, R.: Verifiability experiences in government online voting systems. In: International Joint Conference on Electronic Voting. pp. 248–263. Springer (2017)

Rader, E., Cotter, K., Cho, J.: Explanations as mechanisms for supporting algorithmic transparency. In: Proceedings of the 2018 CHI conference on human factors in computing systems. pp. 1–13 (2018)

Redmiles, E.M., Kross, S., Mazurek, M.L.: How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 1326–1343. IEEE (2019)

Ringle, C.M., Wende, S., Becker, J.M.: Smartpls 4. http://www.smartpls.com (2022)

Saldanha, D.M.F., SILVA, M.B.D.: Transparency and accountability of government algorithms: the case of the brazilian electronic voting system. Cadernos EBAPE. BR 18, 697–712 (2020)

Schmidt, P., Biessmann, F., Teubner, T.: Transparency and trust in artificial intelligence systems. Journal of Decision Systems 29(4), 260–278 (2020)

Sindermann, C., Rozgonjuk, D., Solvak, M., Realo, A., Vassil, K. Internet voting: the role of personality traits and trust across three parliamentary elections in estonia. Current Psychology 42(30), 26555–26569 (2023)

Solvak, M.: Does vote verification work: usage and impact of confidence building technology in internet voting. In: International Joint Conference on Electronic Voting. pp. 213–228. Springer (2020)

Song, C., Lee, J.: Citizens' use of social media in government, perceived transparency, and trust in government. Public Performance & Management Review 39(2), 430–453 (2016)

Spycher, O., Volkamer, M., Koenig, R.: Transparency and technical measures to establish trust in norwegian internet voting. In: International Conference on E-Voting and Identity. pp. 19–35. Springer (2011)

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A.H., Alvarez, R.M.: The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. Government information quarterly 33(3), 453–459 (2016)

Volkamer, M., Kulyk, O., Ludwig, J., Fuhrberg, N.: Increasing security without decreasing usability: A comparison of various verifiable voting systems. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). pp. 233–252 (2022)

Volkamer, M., Spycher, O., Dubuis, E.: Measures to establish trust in internet voting. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance. pp. 1–10 (2011)

Yang, X.J., Unhelkar, V.V., Li, K., Shah, J.A.: Evaluating effects of user experience and system transparency on trust in automation. In: 2017 12th ACM/IEEE International Conference on Human-Robot Interaction (HRI. pp. 408–416. IEEE (2017)

Zollinger, M.L., Estaji, E., Ryan, P.Y., Marky, K.: "just for the sake of transparency": Exploring voter mental models of verifiability. In: International Joint Conference on Electronic Voting. pp. 155–170. Springer (2021)

A. Appendix

Table 1: Participants demographic attribute

Attributes	Dist	Freq	Per
Gender	Female	245	49
	Male	252	50.4
	Non-binary	3	0.6
Age	18-30	130	26
	31-40	515	30.2
	41-50	82	316.4
	51-60	68	13.6
	61-70	59	11.8
	71 and above	10	2
Education	High School	179	35.8
	Bachelor's degree	84	41.4
	Master's degree	207	16.8
	PhD	13	2.6
	Others	17	3.4

Table 2: Internal Consistency Reliability

	CR	AVE
Info. availability	0.855	0.597
Remedial	0.842	0.574
Testing	0.778	0.540

Transparency	0.922	0.748
Understandability	0.889	0.616
Mon. and Veri	0.848	0.584

Table 3: Path Coefficients

			Confidence intervals		Significance
	Path Coefficients	p–values	Lower	Upper	(p<0.05)
H1:Info availability->transparency	0.175	0.003	0.066	0.294	Yes
H2:Understandability->transparency	-0.018	0.746	-0.121	0.095	No
H3:Mon. and Veri->transparency	0.217	0.000	0.111	0.325	Yes
H4:Remedial->transparency	0.225	0.001	0.088	0.360	Yes
H5:Testing->transparency	0.217	0.000	0.116	0.319	Yes

Table 4: Significant Path Coefficients

	Path Coefficients	p – values
H1:Info availability->transparency	0.175	0.003
H2:Understandability->transparency	-0.018	0.746
H3:Mon. and Veri.->transparency	0.217	0.000
H4:Remedial->transparency	0.225	0.001
H5:Testing->transparency	0.217	0.000

Note: Significant at $p < .05$

Author Contributions

SA: paper lead; methodology; validation; writing and review; statistical/data analysis

JB: methodology; writing and review

AD: methodology; data analysis; writing and review

OK: methodology; validation; resources; data curation, writing and review; review; statistical/data analysis; researcher; project administration; funding acquisition.

All authors have read and agreed to the published version of the manuscript.

About the Authors

Samuel Agbesi

Samuel Agbesi is a researcher working on electronic government, data science, and machine learning, usability engineering, human-computer Interactions, privacy, security and blockchain. He holds a PhD in election security from Aalborg University.

Jurlind Budurushi

Jurlind Budurushi is a Computer Scientist specialized in Cyber Security and focusing on Security in the Cloud Native Ecosystem, Usable Security and Secure, End-to-End, Verifiable E-Voting Systems. He is currently employed as a Professor of Computer Science at the Baden-Württemberg Cooperative State University Karlsruhe in Germany. He holds a PhD on Usable Security with application on End-to-End Verifiable E-Voting Systemsfrom the Computer Science Department at the Technische Universität Darmstadt.

Asmita Dalela

Asmita Dalela is an independent researcher working on the human and organisational aspects of security and privacy. She is passionate about fast-moving-technology, qualitative analysis, ethnography, and behavioural analysis, as well as understanding user behaviour on data-sharing, privacy and trust. She holds a Master's degree in Techno-Anthropology from the Aalborg University.

Oksana Kulyk

Oksana Kulyk works as an Associate Professor at the IT University of Copenhagen. Her research interests focus on human and socio-technical aspects of cybersecurity and privacy, including but not limited to election technologies, cyber warfare and trust and transparency in security- and privacy-critical technologies. She holds a PhD in cryptographic internet voting protocols from the Computer Science Department at the Technische Universität Darmstadt.

