"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

Samuel Agbesi[1], Asmita Dalela[2], Jurlind Budurushi[13], and Oksana Kulyk[1]

[1] IT Univserity of Copenhagen, Denmark, {sagb,jurb,okku}@itu.dk
[2] asmita.dalela@gmail.com
[3] Qatar University, jurlind@qu.edu.qa

Abstract. Trust in an election system has been commonly recognized as a crucial factor in the adoption of the system and in ensuring that voters as well as participating parties accept the election outcome as legitimate. Ensuring and maintaining such trust, however, can be challenging, particularly in systems that involve advanced technologies – thus, technologies that both present a larger potential attack surface and are less understandable to lay voters. In this paper, we aim to investigate factors that influence voters' trust in election technologies. For this, we have conducted semi-structured interviews with 14 eligible voters in Denmark. In our analysis, we identified a number of perceived risks that voters have towards the use of election technologies, as well as identified 11 themes, representing factors, that we grouped into *technological trust*, *institutional trust* and *others*. From our analysis, we conclude that there is a need in increasing transparency to ensure voters' understanding of the security level provided by election technologies, as well as in involving other stakeholders such as vendors and election authorities in measures to improve trust. We furthermore conclude that technical measures, while necessary, are not sufficient in ensuring trust in election technologies in absence of general trust towards institutions and society as a whole.

1 Introduction

Ensuring public trust in the election process is crucial regarding the legitimacy of the election and the acceptance of its result by the population, in particular by the supporters of losing parties. However, in the growing presence of threats to the election integrity, such as cyber attacks on election infrastructure or disinformation campaigns, it is particularly challenging to establish and maintain trust. These challenges are even exacerbate by the use of election technologies, such as electronic voting, which enable a larger attack surface (e.g. by allowing an attacker to conduct large-scale manipulations, when electronic voting systems are not protected sufficiently) and are difficult to understand for lay voters (e.g. due to lack of transparency).

This paper aims to understand the factors that influence trust in election technologies, which we define as all electronic systems that are used by the election authorities, such as electronic poll books that contain a list of eligible voters within a voting district, electronic voting system, and electronic tallying system. Thereby, we investigate trust towards election technologies in the context of Danish voters. While Denmark is considered a highly digitized country, its use of election technologies has been limited so far. As such, the voters use traditional, paper-based voting, both for authenticating themselves to election officials at the polling station via authorization letter they receive via mail, and for casting their vote via filling out a paper ballot. While technology is used for e.g. aggregating voting results from polling stations, such processes are usually outside of view for voters. The only aspect of Denmark's election system that uses some form of technology that directly involves the voters is the independent parliamentary candidate declaration process, where the candidates can collect voter declarations from eligible voters electronically, to be eligible to participate in the election [25]. This system, however, faced criticism from security researchers who were able to find security vulnerabilities [30]. In 2012 there was an attempt to introduce Internet voting in the national elections upon a request from mayors of 12 municipalities and the Local Government [10]. A team of experts was commissioned to investigate the feasibility of introducing Internet voting in the Danish electoral process. The investigation identified several advantages that could be achieved through the deployment of Internet voting; however, despite these advantages, trust issues were identified as the biggest disadvantage of introducing Internet voting. Therefore, our goal is to investigate such issues in depth, and to use the results of our investigation as a first step in understanding how to build systems that are not only secure but are also trusted by the voters. To achieve this goal we conducted a qualitative study aiming to answer the following research question:

RQ: What influences the trust of Danish citizens regarding the use of election technologies?

We have conducted interviews with 14 individuals in Denmark who are eligible to vote. We have found that even though the election technologies have the variegated nature, our participants perceived the term election technologies as Internet voting in a broader context, suggesting limited awareness about other kinds of election technologies, including the ones currently in use. The themes that emerged from our analysis show that voters are indeed concerned about security risks in election technologies, and that various measures – such as providing verifiability options, assurances from trusted entities, and transparency measures – can mitigate such concerns. At the same time, we find that trust in society and institutions plays a crucial role. Thus, we conclude and recommend that a holistic approach is necessary to establish voters' trust in elections supported by election technologies.

2 Related work

In this section we describe relevant work in terms of general theories on trust in technology, including election technologies, as well as on trust in the context of Danish society.

2.1 Trust in technology

Trust has been commonly defined as the willingness to rely on other parties while being vulnerable to risks [21]. Trust has been studied across various disciplines, focusing on different aspects of trust. For instance, in the field of computer science, research on trust has been focusing on technologies enabling various security measures such as authentication and access control [14]. On the other hand, studies on trust in social and behavioral sciences tend to focus on users' perceptions and attitudes that influence their trust in a particular entity (e.g. person, organisation or technology) [14]. Thus, it is possible that a mismatch exists between technologies used to ensure the trustworthiness of a system and the extent to which these technologies actually create trust among users [24].

In the context of technology, a number of studies have investigated users' perceptions of trust regarding different technologies, such as consumer-generated content [9], AI-based recommendation systems [32], mobile payment platforms [31], e-commerce services [35], online reviews [11], cloud-based systems [18], and IoT systems [15]. These studies have concluded that trust is crucial for the adoption of corresponding technologies, as well as identified factors as transparency of the system, security, privacy, perceived risk, social influence, information quality, and performance efficacy to influence users' trust in the context of technology.

Particularly relevant to our work is the investigation of trust in e-government services. As such, a recent study by Li and Xue [19] analyzed the factors influencing Chinese citizens' trust in the continuous use of e-government systems. The findings of the study showed that factors such as trust in government, trust in the Internet, information quality, and service quality are key factors influencing citizens' trust. The study by Gulati et al. [13] also identified motivation, willingness, competence, benevolence, predictability, honesty, and reciprocity as key factors influencing citizens' trust. Trust in the Internet was also identified by Aranyossy [3] to influence citizens' trust in e-government services. These findings were also supported by [2] and [27]. In the work by Alharbi et al. [2], trust in government, trust in the Internet, and social trust were found to influence citizens' intention to use e-government services. Apart from trust in the government and the Internet, the study conducted by Ranaweera [27] also identified perceived security, perceived privacy, and perceived risk to influence citizens' use of e-government service.

Other studies have focused on researching the role of trust in election technologies. As such, Dalela et al. investigated voters' trust in risk-limited audits, showing that voters had less confidence when informed about the details of the auditing process, namely, the number of ballots chosen to be audited [6]. Zhu et al. [38] identified privacy, security, usability, and validity of election technologies as key factors influencing citizens' intention to use e-voting. Other

factors such as convenience [17,20], ease of use and trust in the Internet [22], level of digitalisation in the society, perceived security of the Internet and voter socio-demographic status [20,8] have also been identified to influence citizens' intention to use election technologies. While these studies have emphasized the importance of trust in the adoption of election technologies, they did not explore what influences voters' individual willingness to trust in election technologies or lack of it. An investigation of some of these factors has been conducted by Ehin and Solvak [7] in the context of Estonian elections via a quantitative study, confirming the effect of voters' political preferences on trust towards Internet voting. We complement their work by conducting an explorative qualitative study, looking into further factors that influence voters' individual trust regarding the use of election technologies in an electoral process.

2.2 Trust in Denmark

Prior studies [33,23] have postulated that there is a high level of trust among Danish citizens, and one of the key factors that have influenced this level of trust within the Danish society has been attributed to the universal welfare state. According to the work by Svendsen et al. [33], the Scandinavian countries, which include Denmark enjoy a high level of social trust because of "institutional quality" and "equal access to public goods" [33], i.e. citizens having equal access to goods and services. Furthermore, the level of social trust in Denmark has also been attributed to the political stability in the country [33]. Political instability can destroy a country's social trust, and Denmark has accumulated this social trust over a period of time due to its stable political system [33].

Apart from the trust among the Danish citizens, there is also trust between the citizens and the authorities. A study conducted by Nilsen and Lindvall [23] during the COVID-19 pandemic showed that citizens had high trust in the authorities and the health officials in providing COVID guidelines. This trust in authorities has also been argued to play a role in citizens' trust in public digital services introduced by the government. Citizens have trust and confidence in the authorities to implement a secure public digital service [36], and this trust has played an important role in the increased use of digital services in Denmark. Nonetheless, despite the trust citizens have in the various digital services, their trust towards election technology and its use in an electoral process has not been systematically studied, yet.

3 Methodology

The main goal of this work is to gain an in-depth understanding of factors that influence citizens' trust in the use of election technologies, and to develop a theory out of themes emerging from the collected data. We followed an inductive approach [29] and conducted interviews with participants (eligible voters in Denmark). To achieve this goal, we developed an interview guide based on previous research, namely [2,37,39]. The guide consists of three sections. In the

first section, we investigated participants' perception regarding online services and their level of trust in these services. We questioned them about their experiences and concerns when using these services. In the second section, we explored participants' perceptions of election technologies by asking questions related to their confidence in the election result in the case of internet voting. Finally, in the third section, we examined participants' trust in election authorities by asking them about the integrity and accountability of the authorities.

Recruitment and Data Collection For our study we recruited participants that are eligible to vote in Denmark, which includes Danish citizens as well as expats who have the right to vote (e.g. in local elections). The participants were selected using purposive sampling, and whether they have voted on any of the elections conducted in Denmark and/or reported having knowledge about the electoral process in Denmark. None of the participants have used e-voting to vote in a political or non-political elections. The participants were contacted and invited to participate in the study via emails and personal phone calls. In total 14 participants took part in our study, consisting of four female and ten male participants. The age of the participants ranged from 18 to 70 years old, and their level of education ranged from High School diploma to Doctorate degree.

In order to collect data we conducted semi-structured interviews. The interviews were conducted either face-to-face or online. Note that the interview guide used to collect the data went through three iterations. In each iteration, we conducted a pilot interview and after the interview the project team meet to discuss and improve the questions based on the responses of the participant. Ambiguous questions were re-worded, and questions that did not add further value to our research were deleted.[4].

Data Analysis In order to analyse the collected data thematic analysis was used. "Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data" [5]. Thematic analysis has been argued to be the appropriate technique for data analysis with respect to qualitative studies, which are not dependent on an initial theoretical framework. This method fits to our research goal of identifying themes from the collected data and using these to design a model with respect to factors that influence voters' trust in election technology. Our thematic analysis follows the steps described by Braun and Clark [5]. The first step was to familiarize with the content and to get a general overview of the collected data by reading through the interview transcripts. This step allowed us to take note of some initial ideas for the second step, namely coding. After the first step, we read through the interview transcripts again, but this time line-by-line. In this second step, extracts from the collected data that appeared interesting regarding our research question were assigned labels, so called codes. The list of codes generated in the second step were then classified. Codes were

[4] The resulting interview guide is available at `https://github.com/cometitu/interviews`

classified into different sub-themes/themes based on their relationship. Finally, the sub-themes/themes were reviewed, and final themes were identified. For our data analysis the NVIVO software package was used.

Reliability and Validity The reliability and validity of qualitative research assesses the rigor and the dependability of the procedures and methods followed during the data collection and analysis [28]. In the context of this study to ensure validity and reliability, we carefully selected interview participants. Furthermore, two other researchers randomly selected five interview transcripts for coding. Most of the codes generated by the two other researches were in line with the codes generated by the principal coder. The variations in the codes were discussed between the three researchers. Afterwards, the aligned codes were classified in sub-themes/themes. Finally, the sub-themes/themes were reviewed by four researchers and final themes were identified.

Ethics Before the beginning of each interview participants were provided with a consent form. In the face-to-face interviews we asked participants to read and fill out the consent form. In the online interviews, we read out the consent form and made sure participant's agreed to it before proceeding with the interview. Participants were assured that all information is used anonymously and only for research purposes. To ensure participants' anonymity, we removed all identifiable information that appeared in the interview transcript.

Study Limitations The study has some limitations. Most of the individuals that we interviewed were located in the capital city and had at least a Masters degree. Hence, it is not clear to which extent the findings can be generalized, e.g. to Danish voters in rural areas or to voters with lower levels of education. Even though our sample is considered sufficient for an exploratory, qualitative study [4,26], further large-scale studies need to be conducted in order to better understand to which extent our findings are common in a representative population.

4 Results

This section reports our findings from the data analysis[5]. First, we present the findings with respect to the perceived risks regarding election technologies. Since risk and trust are inextricably intertwined, that is, if no risk is perceived, then there is no need for trust. Therefore, it is important to look at factors that constitute perceived risk in our analysis. Afterwards, we introduce the factors that influence voters' trust regarding election technologies.

[5] The codebook containing the summary of derived codes and their frequences are available at `https://github.com/cometitu/interviews`

4.1 Perceived Risks

Our analysis shows that participants are aware and concerned about a variety of risks that election technologies can introduce in the election process. Since risk plays a significant role in establishing trust, it is important to discuss what constitutes the perceived risk.

Some participants (5 out of 14) mentioned that the introduction of election technologies in elections will lead to *hackers attack* as it is much easier to hack a thousand computers than to hack a thousand people. The participants also emphasized that the security of Big tech companies has been compromised in the past, therefore it will be easy for hackers to compromise the security of election technologies, if used in Danish elections: *"Even the biggest companies you know Sony, Microsoft, Google, Facebook, they all got hacked. Why would the state of Denmark be any better than those companies in maintaining you know their IT security."* Participants expressed that the risk of hacker attacks could make people insecure regarding the voting process. This would lead to voters' lack of trust in the election system.

Some participants (4 out of 14) mentioned that *manipulation of election results* could happen if election technologies are used. They argued that since a small group of people will be involved in the process, it could be easy to manipulate the election results. For instance, vote secrecy can be violated publishing online voters' preferences: *"In a digital voting system the amount of people involved would be much smaller and closer group where actually the risk for conspiracy or carteling would be... I think it would be easier to make conspiracy with the digital voting system."* Participants highlighted that this will create doubt in citizens' mind around the election results and make them distrust the election system. Further concerns were raised by some participants (5 out of 14) regarding possible *cyber attacks by nation states* and *cyberwarfare*. Thereby, participants expressed that the use of election technologies in Danish elections could make the elections vulnerable to cyber attacks. Malicious actors could try to influence the political scene in Denmark by manipulating the election results: *"We're talking Ukraine cyber war or pressure from Russia and if there's one thing we can do to expose ourselves towards like a Russian influence, that's by having an electronic voting system."*

A few participants (2 out of 14) expressed that *election technologies introduce points of failure* in the system. This can disrupt elections and make voters skeptical of casting their vote: *"If my vote is just a number in a database essentially, then the database is like a single point of failure, which could be influenced and that would make me suspicious."* In addition to the aforementioned factors of perceived risks regarding election technologies, participants raised concerns regarding the *reliability* of such technologies and the possibilities of flaws which could affect the election due to its complexity: *"There will be some, you know there will be places of failure where it could fail more catastrophically. Also, reliability, let's say you have a power cut in the middle of an election."*. Some participants (4 out of 14) expressed that the paper-based systems would be more robust and effective in eliminating such flaws: *"I think there are flaws in every technology*

and I think it would take quite a while before I personally would trust that this [election] technology would be working as it should."

4.2 Factors of Trust

When considering factors that could potentially mitigate or exacerbate the aforementioned risks, influencing the voters' trust in the election technologies – we distinguish between factors related to *Technological*, *Institutional*, and *Other* aspects of trust. All the factors are summarised in Figure 1

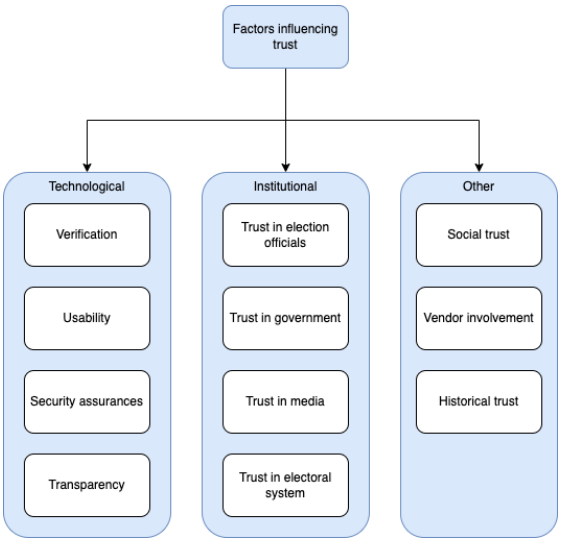

Fig. 1. Factors influencing voters' trust towards election technologies.

Technological Trust Technological trust describes the technical aspects that influence the voter's trust in the use of election technologies, related to the implementation and management of the used IT systems, as well as the communication with the voters regarding the status of these systems. Since election technologies have a significant reliance on IT systems, it is important to understand what technical dimensions contribute to this trust. The main sub-themes we identified hereby include *Verification*, *Usability*, Security Assurances and *Transparency*. We outline each of these sub-themes in the subsections below.

Verification When it comes to the use of election technologies, many participants (8 out of 14) expressed the need of verifying the election results, mentioning concepts such as system audit, verification or traceability. *"I would have confidence in the results, because I would trust that there would be so many verification*

processes of the result." Furthermore, participants expressed the importance of enabling voters to trace their votes. They argued that it is easier to ensure this with the current paper-based voting system because once you mark or cross your intention on the ballot paper it can no longer be altered, but the same cannot be guaranteed when using electronic voting system: *"it is very difficult for you to go back and establish what is called to establish intent of the voter... but for, in the paper I mean, once it is marked, it is marked, you know, that this person, this is whom he or she intended to vote for."*

Usability When it comes to usability of the election technologies, many participants (7 out of 14) emphasized the *ease of use* and the *rules and steps* to be followed while voting electronically, and that these *should be clearly stated*: *"But I will advise that in case the steps, you know, or the rules in voting electronically must be clearly stated so that one can easily go through and follow the steps and vote electronically."*

Security Assurances Half of the participants (7 out of 14) mentioned the necessity of *proper approaches*, i.e. procedures and techniques, when implementing the security assurances in election technologies: *"If implemented correctly and with certain security techniques, it should be more trustable than the current one."* Participants also emphasized that the *enhanced security design* of such technologies will help to restrain tampering of the election outcome: *"What will make me trust or not trust will depend upon how secure the technology is, you know, so if the security features are very well enhanced or are very strong such that the, our voting can not be in any way tampered electronically."* Some participants (4 out of 14) mentioned *authentication* as an important security assurance to influence the voters' trust in election technologies. Participants proposed the use of different authentication techniques such as secure login code, NemID or social security number to prevent unauthorized login into the voting platform: *"There should be a security or some sort of private code that pertains to everybody individually, such that it is known to you alone, that you can be able to use to enter into the system and vote."*

In addition to the need of following proper security approaches, many participants (7 out of 14) mentioned different kinds of assurances made on behalf of election authorities and other experts regarding the security of election technologies. Participants highlighted that elections authorities such as government official or representatives of opposing parties can convince voters regarding the safety and security of an election technologies which can lead to trust: *"Yes, I will feel confident if and only if, you know, before the vote is being cast... they are able to explain all the authorities concern are able to explain how secure the system is or how secure the e-voting is going to be."*

Apart from assurances by government officials, assurances from academic researchers and other professionals about the security of election technologies were also mentioned to influence voters' trust. Some participants (3 out of 14) stated that they trust these experts to investigate and determine the security of these technologies and also provide a solution that can make it more secure: *"I*

think for me personally, it would have to be a matter of like scholarly investigation of how to secure such a process. "

Transparency Transparency, also emerged as one of the main influencing factors of voters' trust in election technologies, as it is the need for the voters to be able to follow the workings of the election technologies. Participants (6 out of 14) revealed how the lack of transparency can have a negative effect on citizens' trust. In particular, one participant felt that an inherent disadvantage of election technologies is that it is designed as a black-box, so that lay voters are unable to understand how the system works – an issue that can be misused by a party that may want to create mistrust in the election outcome: *"It would be easier for the loser of the election to blame the loss on something that's been happening inside of this black box."* The raised issue with transparency in election technologies was contrasted with the paper-based voting process that was assumed to be easier to follow for every voter: *"I think from the general population have very little understanding of how a system like this would work, and it's easier to kind of visualize and understand how it works when you vote on paper."*

Institutional Trust Institutional trust describes the inherent trust of voters in the election officials, the government, media, and the electoral system. During the interviews it was evident that the collective trust in these entities creates a positive impression in the participant's mindset and convinces them to adopt the use of election technologies in the future elections. The main sub-themes include *Trust in Election Officials*, *Trust in Government*, *Trust in Media*, and *Trust in Electoral System*. We outline each of these sub-themes in the subsections below.

Trust in Election Officials Many participants (7 out of 14) mentioned that they believe in the integrity of the election officials and expect them behave according to the electoral law: *"I will just give them the benefit of the doubt that they will do something good."* Participants highlighted that the inclusion of diverse group of people from different demographics provides enough validation to maintain their collective integrity. The fact that the officials are the chosen representatives from all the parties participating in the election, ensures a positive mindset in the voters that a *self regulated system is maintained inside the system*: *"I would trust them because they are the people that are sitting there and taking the roles, they are elected by the local government within all parties. As far as I know, these are people from all parties. "* Participants mentioned also that there have never been any complaints or fraud that have surfaced which can make them question their trust in the officials: *"I have not heard any complaint. The last election that I participated in, I didn't heard any complaints or fraud."* When it comes to the implementation of election technologies, the technical competence of the election officials is also a driving factor for the acceptance and trustworthiness of the technologies by the voters. Many participants (7 out of 14) mentioned election authorities' lack of technical expertise for implementing such technologies and therefore they don't trust them to be able to run and

maintain such systems effectively. The participants conveyed their trust in the integrity of the election officials, however, they were sceptical of their technical competences: *"I can trust them to be honest. Right. I don't think I can trust them to be competent."* Participants also emphasized that it will be beneficial if some experts who have competence regarding election technologies can help the election officials in developing and maintaining such systems: *"Our authorities, I'm not sure that anyone there actually understands what it would take to make such a system, so we would have to have experts somewhere from where they have some good understanding of how such systems could run and and be created, I think."*

Trust in Government Some participants (4 out of 14) mentioned that they will trust the government decision to implement election technologies as they believe that the government will undertake proper testing and verification measures into consideration before implementing any new technology for future elections. Participants feel that government will assure the voters that the technology is reliable and secure to be used in elections, see also Section 4.2, for a discussion of a related theme of security assurances): *"I will say I trust it because this is recommended from government or from the politicians or whatever because and then we trust that this is OK because I would assume that there would be made so many testing and verification."* Participants also emphasized that the government is bound to take the right measures as any mishandling will be projected by the opposition party, which will create a negative image for the governing party in the voters: *"I may not have any mistrust issues when it [mishandling] happens that the opposing parties, I mean the losing parties start to complain and point out valid [arguments]."*

Trust in Media A few participants (3 out of 14) articulated that they have trust in media for creating news and exposing the mishandling of the data if that happened during the implementation of the technologies. Thus, avoiding potential corruption or cheating. Participants have a firm belief that the media will make sure that any discrepancy is reported to the voters: *"In Denmark, everything would be exposed if somebody tried to cheat the system, they would be exposed and they would rather they will be expelled of the system."*

Trust in Electoral System Participants (4 out of 14) mentioned that they have confidence in the Danish electoral system and believe that it works efficiently due to an involvement of diverse group of people from different parties making it difficult to forge a conspiracy. Participants also mentioned that new election technologies will not create any added value for them to trust more the election system: *"There's already trust in the electoral system itself, so I'm not sure that there is the need to introduce technology in order to create more trust."*

Others A number of further factors were identified that could not be clearly grouped into technological or institutional trust, although being related to the fac-

tors from these categories. These factors include *Social Trust*, *Vendor Involvement*, *Historical Trust*.

Social Trust Social trust examines how trust within Danish society influences voter's trust in election technologies. A few participants (3 out of 14) mentioned that the general trust in the society can play an important part in influencing the use of election technologies. Participants emphasized that without this general trust it will be difficult to adopt election technologies: *" So if there is general trust in society, then there is likelihood that I will trust, but if there is mistrust in the society, then there's the likelihood that I will also mistrust whatever outcome."* This general trust in the society also gives the confidence to the voters that in case of any mishandling on the part of election authorities – it will be reported: *"I have confidence in that if there is anything Wrong, someone will lift the finger and say hey, we have to look at this So that gives me a high degree of trust."*

Vendor Involvement The vendor involvement in implementing election technologies emerged as a significant theme during the interviews as some participants (5 out of 14) mentioned the need of secure technology as the key for executing fair elections. It became evident from the interviews that the voters distrust the vendors of election technologies. Participants believe that the security of the election technologies may get compromised if there is an involvement of vendors in developing, executing and managing these technologies. They emphasized on the need of developing technology internally to avoid potential security issues and data-breaches since election is a high-stake event: *" if you're designing own systems from scratch, you are not in trouble. If you are like allowing a private entity to, to control the information. Okay. That's problematic."* Participants also expressed that the vendors are just eager to sell the technology and don't do enough due-diligence when it comes to developing secure technologies. They also have a skepticism that the vendors could potentially sell the confidential information to the third-parties: *"You know the vendors and the kind of details they have about me. What they are going to use it for. It will be a kind of a worry to me."* A few participants (2 out of 14) also emphasized that vendors pedigree impacts their trust in election technologies. They articulated that it is important for them to know the vendor's affiliation with and reputation in Denmark: *"if I know that it is a Danish company, then I will assume that the kind of trustworthy that we have in this society would be translated into the voting and for that I'm secured."* A few participants (2 out of 14) mentioned that the affiliation of vendors with the Nation State could lead to privacy risk and manipulated election results. Therefore, it is important for them to know the vendor's intent so that the trust in their proposed technology can be established: *"you can't tell me that, OK, the company behind these technologies, coming from, let me see Russia or China right that has some kind of issues with privacy and also trustworthy instantly. I will not feel secured because I know my data will be used for other purpose or maybe they might even manipulate results."*

Historical Trust Our analysis revealed that participants have made a deep connection with the paper-based voting system and have complete trust in it. Some participants (4 out of 14) mentioned that since the paper-based system works well, there is no need to use election technologies. They prefer using the paper-based voting system as they find it less risky and more reliable: *"'cause I'm like what is wrong with the [paper based] system as... I don't see the current election process as broken. So I'm like what is it that needs fixing?"*

5 Discussion and Conclusion

Our findings confirm the importance of trust regarding voters' acceptance of election technologies, in particular when related to perceived security. The study's participants were aware of threats related to the use of technology in elections, and perceived these to be higher when compared to the paper-based systems. Predominantly participants mentioned general concerns, but only few specific to election technologies, namely election manipulation and denial of service attacks. Other threats, such as violation of vote secrecy, voter coercion, and vote buying were not mentioned. This shows either participants' lack of awareness or lack of concerns towards these threats.

Factors identified in our study, especially those relating to trust in technology, point to potential measures that can be taken to increase voters' trust in a specific election or a specific voting system. For instance, our participants point to the need of verifying the election result, confirming the need to use end-to-end verifiability (as opposed to black box systems) commonly pointed to also by experts [34]. Verifiability, in addition to providing a layer of security assurance regarding election integrity, can also serve as means for engaging the voter. It enables voters to experience security-related aspects of the system, and makes the system potentially more transparent. These and other measures of involving the voter can be used to enhance *transparency* of election technologies, which was another issue commonly mentioned by our participants. Indeed, ensuring transparency when using technology in elections is a known challenge, which has also been at the core of the German Constitutional Court decision regarding the use of electronic voting machines [12]. Effective ways to ensure transparency as a way to establish trust remain an open question, especially in light of studies showing that providing too much information about the technology without properly contextualising it might even lead to decreased confidence in the election integrity [6]. A significant role in ensuring some degree of transparency – assuming that lay voters do not have the expertise necessary to understand the details of how election technologies work – lies within security assurances presented by trusted entities, such as election authorities, representatives from opposing parties or independent experts.

With respect to various stakeholders involved in the election, our participants expressed high trust regarding the integrity of election officials. However, some doubted their expertise in implementing and administrating election technologies. Such, seemingly conflicting views point to the manifold nature of trust, in

particular, to both perceived integrity/benevolence and perceived competence being crucial to trusting intention [21]. While perceived integrity depends strongly on the general level of trust in society, competences of election authorities can be improved with corresponding training and/or by involving experts as consultants. The introduction and use of such measures should be communicated to the voters in a transparent manner. Our participants were less convinced of the trustworthiness of vendors who implement election technologies, doubting their commitment to the security of their products. Similar scepticism towards the intentions of private companies to ensure sufficient security and privacy protection has also been shown in other domains [15,16], thereby emphasising the importance of independent institutes (e.g. media reporting), appropriate legislation, and independent audits for security-critical systems. Transparent processes when procuring election technologies, including proper vetting and oversight over vendors, is therefore crucial.

When talking about election technologies, our participants mainly talked about Internet voting, which might be due to lower awareness about other technologies that are or can be used in the electoral process. Therefore, it remains an open question to which extent identified factors that influence trust in Internet voting are relevant to other kinds of election technologies, such as party endorsement system, electronic voter register or software used for tallying cast votes. While some of these factors are likely to be transferred directly, such as trust in government, other might require a more nuanced approach. In particular, applications of verifiability techniques to processes such as endorsing a party to be eligible for being elected can be relevant, especially in light of identified attacks on such processes in Denmark [30]. Studying such techniques as well as voters' attitudes towards them can be a worthwhile direction of future work.

A number of factors identified in our study were not connected to a specific technology or voting system. These factors pointed at the attitudes towards institutions and society as a whole, confirming findings by previous works [1,19]. This means that improving technology can only solve the problem of citizens' trust to a limited extent. Essentially, unless there is already a high level of social trust and trust in the governmental institutes, it is likely that the use of technology will fail.

Future Work We consider following directions to be particularly interesting for future research. As our study focused on the voters in Denmark, similar studies in other countries – especially countries characterised either by lower levels of social trust or more extensive use of election technologies compared to Denmark – would help to better understand how voters' trust is established and maintained. While our study was qualitative and served an exploratory purpose, further quantitative, large-scale evaluations can be used to validate and to elaborate our findings. Finally, ways to engage voters and other stakeholders in trust-building measures – including but not limited to the development and evaluation of usable verifiability measures, awareness materials and explanations of the security guarantees that election technologies provide – should be investigated.

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

References

1. Alharbi, A., Kang, K., Hawryszkiewycz, I.: The influence of trust and subjective norms on citizens' intentions to engage in E-participation on E-government websites. ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems (2015)
2. Alharbi, N., Papadaki, M., Dowland, P.: The impact of security and its antecedents in behaviour intention of using e-government services. Behaviour and Information Technology **36**(6), 620–636 (2017). https://doi.org/10.1080/0144929X.2016.1269198
3. Aranyossy, M.: Citizen adoption of e-government services-evidence from hungary. In: Bled eConference. p. 39 (2018)
4. Boddy, C.R.: Sample size for qualitative research. Qualitative Market Research: An International Journal (2016)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology (2006). https://doi.org/10.1191/1478088706qp063oa
6. Dalela, A., Kulyk, O., Schürmann, C.: Voter perceptions of trust in risk-limiting audits. E-Vote-ID 2021 p. 335 (2021)
7. Ehin, P., Solvak, M.: Party cues and trust in remote internet voting: Data from estonia 2005–2019. In: International Joint Conference on Electronic Voting. pp. 75–90. Springer (2021)
8. Faraon, M., Stenberg, G., Budurushi, J., Kaipainen, M.: Positive but skeptical: A study of attitudes towards internet voting in sweden. In: CeDEM Asia 2014: International Conference for E-Democracy and Open Government, Hong Kong, December 4-6, 2014. pp. 191–205 (2015)
9. Filieri, R., Alguezaui, S., McLeay, F.: Why do travelers trust TripAdvisor? Antecedents of trust towards consumer-generated media and its influence on recommendation adoption and word of mouth. Tourism Management **51**, 174–185 (2015). https://doi.org/10.1016/j.tourman.2015.05.007
10. Folketinget: Technical dialogue on system for e-voting in denmark-summary report (1 2013), https://www.ft.dk/samling/20121/lovforslag/l132/bilag/1/1209863.pdf
11. Furner, C.P., Drake, J.R., Zinko, R., Kisling, E.: Online Review Antecedents of Trust, Purchase, and Recommendation Intention: A Simulation-Based Experiment for Hotels and AirBnBs. Journal of Internet Commerce **21**(1), 79–103 (2022). https://doi.org/10.1080/15332861.2020.1870342
12. German Federal Constitutional Court: Decisions: Order of 03 march 2009 - 2 bvc 3/07 (2009)
13. Gulati, S., Sousa, S., Lamas, D.: Modelling trust: An empirical assessment. In: IFIP Conference on Human-Computer Interaction. pp. 40–61. Springer (2017)
14. Hoffman, H., Söllner, M.: Incorporating behavioral trust theory into system development for ubiquitous applications. Personal and ubiquitous computing **18**(1), 117–128 (2014)
15. Kulyk, O., Milanovic, K., Pitt, J.: Does my smart device provider care about my privacy? investigating trust factors and user attitudes in iot systems. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. pp. 1–12 (2020)

16. Kulyk, O., Renaud, K.: "i need to know i'm safe and protected and will check": Users want cues to signal data custodians' trustworthiness. In: 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW). pp. 171–178. IEEE (2021)
17. Kulyk, O., Volkamer, M., Fuhrberg, N., Berens, B., Krimmer, R.: German voters' attitudes towards voting online with a verifiable system. In: Workshop on Advances in Secure Electronic Voting (VOTING), Grenada, February 18, 2022 (2022), 46.23.01; LK 01
18. Lansing, J., Sunyaev, A.: Trust in cloud computing: Conceptual typology and trust-building antecedents. Data Base for Advances in Information Systems **47**(2), 58–96 (2016). https://doi.org/10.1145/2963175.2963179
19. Li, W., Xue, L.: Analyzing the Critical Factors Influencing Post-Use Trust and Its Impact on Citizens' Continuous-Use Intention of E-Government: Evidence from Chinese Municipalities. Sustainability (Basel, Switzerland) **13**(14), 7698 (2021). https://doi.org/10.3390/su13147698
20. 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: International Joint Conference on Electronic Voting. pp. 91–105. Springer (2021)
21. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. The Academy of Management Review (1995). https://doi.org/10.2307/258792
22. Nemeslaki, A., Aranyossy, M., Sasvári, P.: Could on-line voting boost desire to vote?–technology acceptance perceptions of young hungarian citizens. Government Information Quarterly **33**(4), 705–714 (2016)
23. Nielsen, J.H., Lindvall, J.: Trust in government in sweden and denmark during the covid-19 epidemic. West European Politics **44**(5-6), 1180–1204 (2021)
24. Nissenbaum, H.: Will security enhance trust online, or supplant it? Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions, Eds. R. Kramer and K. Cook, Russell Sage Publications (2004) pp. 155–188 (2004)
25. OSCE: Denmark, general elections, 5 june 2019: Needs assessment mission report (6 2019), $https://www.osce.org/files/f/documents/4/d/419231_0.pdf$
26. Plano Clark, V.L., Creswell, J.W.: Understanding research: A consumer's guide (2015)
27. Ranaweera, H.M.B.P.: Perspective of trust towards e-government initiatives in Sri Lanka. SpringerPlus **5**(1), 22 (2016). https://doi.org/10.1186/s40064-015-1650-y
28. Roberts, P., Priest, H.: Reliability and validity in research. (2006). https://doi.org/10.7748/ns2006.07.20.44.41.c6560
29. Saunders, M., Lewis, P., Thornhill, A.: Research methods for business students. Pearson education (2009)
30. Schürmann, C., Bruni, A.: Technical and socio-technical attacks on the danish party endorsement system. In: International Joint Conference on Electronic Voting. pp. 200–215. Springer (2019)
31. Shao, Z., Zhang, L., Li, X., Guo, Y.: Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. Electronic Commerce Research and Applications **33**(August 2018), 100823 (2019). https://doi.org/10.1016/j.elerap.2018.100823, https://doi.org/10.1016/j.elerap.2018.100823
32. Shi, S., Gong, Y., Gursoy, D.: Antecedents of Trust and Adoption Intention toward Artificially Intelligent Recommendation Systems in Travel Plan-

ning: A Heuristic–Systematic Model. Journal of Travel Research **60**(8), 1714–1734 (2021). https://doi.org/10.1177/0047287520966395, https://doi.org/10.1177/0047287520966395
33. Svendsen, G.L.H., Svendsen, G.T., Graeff, P.: Explaining the emergence of social trust: Denmark and germany. Historical Social Research/Historische Sozialforschung pp. 351–367 (2012)
34. 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)
35. Wang, S.W., Ngamsiriudom, W., Hsieh, C.H.: Trust disposition, trust antecedents, trust, and behavioral intention. Service Industries Journal **35**(10), 555–572 (2015). https://doi.org/10.1080/02642069.2015.1047827
36. Yasuoka, M., Meyerhoff Nielsen, M., Iversen, K.E.: The exercise of mandate–how mandatory service implementation promoted the use of e-government services in denmark. In: Proceedings of the 55th Hawaii International Conference on System Sciences (2022)
37. Zada, P., Falzon, G., Kwan, P.: Perceptions of the australian public towards mobile internet e-voting: risks, choice and trust. Electronic Journal of e-Government **14**(1), pp117–134 (2016)
38. Zhu, Y.Q., Azizah, A.H., Hsiao, B.: Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries. Information Development **37**(2), 193–208 (2021). https://doi.org/10.1177/0266666920902819
39. Zhu, Y.Q., Azizah, A.H., Hsiao, B.: Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries. Information Development **37**(2), 193–208 (2021)