Investigating State-of-the-Art Practices for Fostering Subjective Trust in Online Voting through Interviews

Karola Marky, *Leibniz University Hannover and University of Glasgow;*
Paul Gerber and Sebastian Günther, *Technical University of Darmstadt;*
Mohamed Khamis, *University of Glasgow;* Maximilian Fries and
Max Mühlhäuser, *Technical University of Darmstadt*

https://www.usenix.org/conference/usenixsecurity22/presentation/marky

This paper is included in the Proceedings of the
31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the
31st USENIX Security Symposium is
sponsored by USENIX.

Investigating State-of-the-Art Practices for Fostering Subjective Trust in Online Voting through Interviews

Karola Marky
Leibniz University Hannover, University of Glasgow

Paul Gerber
Technical University of Darmstadt

Sebastian Günther
Technical University of Darmstadt

Mohamed Khamis
University of Glasgow

Maximilian Fries
Technical University of Darmstadt

Max Mühlhäuser
Technical University of Darmstadt

Abstract

Ensuring voters' subjective trust is key to adopting any voting system. Consequently, researchers, experts, and policymakers have proposed and implemented practices to foster the trust of voters in online voting. State-of-the-art practices include security features, public information, or evaluations. However, it remains unclear how these practices affect the voters' subjective trust. Through interviews with 26 participants, this work presents the first analysis of voters' perceptions considering state-of-the-art practices that help voters determine their trust in Internet voting. Among our results, we show practices, such as expert evaluations, that we identified as mandatory. Further, we found practices, such as individual verifiability, that facilitate trust. Others, such as vote updating, have a negative impact due to unfamiliarity. We, furthermore, report misconceptions, discuss ways to address them through different information interfaces or as part of the voting software. Finally, we list recommendations for the specific realization of expedient practices to inform developers and policymakers.

1 Introduction

Elections form the basis of democracies. With the drive to global digitization, some countries [22] offer online voting based on several benefits, such as decentralization of vote casting, cost reduction, or faster announcement of the election result. Furthermore, such benefits might result in more frequent elections and polls in communities, creating opportunities for more citizen participation and collaborative decision-making.

The realization of online voting requires secure systems that consider human factors simultaneously. While security properties (e.g., [3, 30, 65, 66]) as well as usability (e.g., [43, 79]) were thoroughly investigated, there is another key component that is required for realizing online voting: subjective trust of voters [53, 73, 75]. Without subjective trust, benefits from online elections are not evident since voters will not use the online voting system [12, 48, 53, 58]. Furthermore, trust is crucial for accepting the phase of vote tallying [47]. This can also be evidenced in countries that already offer online voting, such as Estonia or Switzerland. Even though security features of existing online voting schemes are continuously updated – for instance, by introducing verifiable cryptographic shuffling of votes [31, 57] – and individual verifiability is offered, missing trust forms a barrier to adopting online voting [13, 17, 40, 46].

Subjective trust can be decomposed into dispositional trust, learned trust, and situational trust [52]. *Dispositional* trust refers to a voter's general propensity to trust others rooted in personality; hence it cannot be influenced by a government or other agency [7]. *Learned* trust is based on past usage experiences with a voting system [52]. In this scope, user experience has been demonstrated to be important [43]. However, voters have to interact with a voting system to build learned trust. Finally, *situational* trust is based on situational cues which can be given by available information or societal expectations [44, 52]. Consequently, such situational cues are crucial for the subjective trust assessment of voters who have never used an online voting system before.

In this paper, we investigate the following main research question: How do state-of-the-art practices that aim to help voters determine their subjective trust when participating in online elections impact the voters' trust perceptions? For this, we assume that the provided online voting system follows democratic and security standards. To foster situational trust, researchers, experts, and policymakers suggested a range of different practices to assist voters in gaining information throughout the entire electoral process [71]. Several of these practices have been realized in countries that allow online voting, such as Estonia, and countries that tested online voting, e.g., Norway. Examples of realized practices include expert evaluations of the voting software [6], or the disclosure of source code [56].

However, it remains unclear how such practices contribute to the adoption of online voting systems. To investigate this topic, we collected nine groups of state-of-the-art practices by reviewing the literature and practices in countries that permit online voting. Through an interview study (N=26),

we evaluated how those nine state-of-the-art practices are perceived in terms of subjective trust.

Based on previous work, we followed a deductive approach to cluster the practices into four groups (1) mandatory, (2) positive, (3) neutral, and (4) negative practices, based on their impact on subjective voter trust. Furthermore, we identified misconceptions connected to the practices and new practices with the potential to foster subjective trust.

Our results show that simply executing the practices is not enough since information about them and the involved entities, e.g., institutions, are also crucial elements. Based on our results, we discuss factors that impact the realization of each practice and further contribute by giving recommendations on the realization and implementation of interfaces that communicate the practices to voters. Based on our findings, we discuss factors that impact the realization and implementation of information interfaces and voting software to support policymakers and developers to increase voters' trust in online voting systems.

Contribution Statement. While previous work primarily focused on either online voting as a generic concept or specific online voting implementations, we contribute an investigation of how and why state-of-the-art trust practices impact the trust perceptions of individuals. Our results serve as a stepping stone to create practices and interfaces that are needed when introducing online voting as new voting channel. We further identify misconceptions that negatively impact trust and discuss means to address those. Based on our results, we provide recommendations for 1) implementing trust practices in real elections focusing on the introduction of online voting and 2) information interfaces for voters.

2 Background & Related Work

In this section, we first detail trust definitions and theories before we give an overview of existing related work that investigated aspects of e-voting trust in the past.

2.1 Trust Definitions and Theories

There are several definitions of trust in the literature. In this paper, we use the definition by Marsh and Dibben [44] because it is specifically tailored to technology use, which is as follows: *"Trust concerns a positive expectation regarding the behavior of somebody or something (the trustee) in a situation that entails risk to the trusting party (the truster)"*. The presence of risk is essential for trust [10]. In the context of online voting, there are two main risks. First, the voting choice might be revealed to another party. Second, the election might be manipulated such that other candidates not chosen by the voters win. Therefore, voters must have the opportunity to determine their subjective trust in an online voting system.

Determining trust in the context of the Internet is more challenging for users compared to the physical world [52]. Consequently, the level of trust imposed by individuals might not match reality. Overtrust can be exploited for different kinds of attacks, such as phishing [34] or tricking voters into using insecure voting systems. If trust is too low, individuals might avoid Internet-based solutions that add convenience or other benefits to their daily lives [23]. Too low trust levels might either result in users untrusting or distrusting a technology [45]. In the context of online voting, untrust might lead potential voters not to use the provided online voting system. Distrust, however, could mean that voters demonstrate against an online voting system or even try to sabotage it. Trust can change over time, starting with initial trust that emerges into an exchange of information, finally leading to a long-term trust assessment [63]. Introducing online voting would require authorities to constantly provide adequate information for voters to enable transparency. The nature of trust has multiple dimensions: dispositional trust, learned trust, and situational trust [52]. Since dispositional trust of voters is based on their personality, voting authorities cannot impact it even though dispositional trust impacts the willingness to use online voting [13]. Learned trust is based on past experiences with a voting system and the authorities that provide it. Voters who tried online voting once will likely use it again [70]. Hence, if voting authorities wish to support voters in determining trust, situational trust is the only component that they can target.

For online voting to be successful, it has to be adopted by a particular share of the electorate. Roger's theory of diffusion of innovation (DOI) is a well-established and comprehensive model that considers technology adoption based on five dimensions: 1) relative advantage over previous technology, 2) complexity, 3) compatibility, 4) trialability, and 5) observability [59]. Five practices investigated in this work specifically target two dimensions of the DOI: The DOI dimension of trialability is how technology can be experimented with and whether online voting trials are possible. Second, observability is the visibility of new technology, which considers to which degree the results of using online voting are visible. The DOI has partly been applied to online voting by Carter *et al.* [13] who found dispositional trust and the dimension relative advantage, i.e., the benefit of using online voting compared to existing voting channels, to impact adoption.

2.2 Trust in E-Voting

In this section, we describe related work that mentions subjective trust in the scope of e-voting. The subjective trust of voters is crucial for accepting e-voting in general, which has been shown all over the world [48, 53, 58]. E-Voting in the form of voting computers in polling places was used in Kazakhstan but discontinued due to trust issues [37]. Similar trust issues were shown in Bahrain [5] and Palestine [62]. However, trust might be connected to the specific culture. In Nigeria,

for instance, the usage of e-voting contributed to trust [51]. Zhu *et al.* report an experiment with 426 Indonesian voters and show that subjective trust is related to security, usability, privacy, and validity aspects [77]. Several countries, such as the US and India, currently use voting computers and have done pilots in the past. An analysis of e-voting pilots in the UK revealed that perceived trust is not only influenced by security but also by provided verification options, staff training, and the legislative framework [76].

Considering trust in the context of e-voting, related work either investigated trust perceptions of specific systems that are or were used in practice or trials. These trust perceptions are mostly related to the specific functionality of the technology that is provided, legislation, and the training of poll workers. The impact of trust practices –as defined in Section 3– on the voters' subjective trust was not investigated.

2.3 Investigations of Trust in Online Voting

Several publications investigated subjective trust in online voting systems. Carter and Bélanger specifically investigated factors that contribute to the intention of use [12]. Among complexity and compatibility as constructs from the DOI, perceived trustworthiness was an essential factor. Carter *et al.* [13] further investigated Internet voting in the context of DOI through a survey with 372 participants specifically considering relative advantage, accessibility and compatibility. Further, institution-based trust and dispositional trust were investigated. Dispositional trust and the relative advantage that online voting offers impact adoption. The research presented by Carter *et al.* considers online voting as a generic concept without considering specific realizations or systems.

The research by Milic *et al.* is most closely connected to ours [46]. They specifically investigated the subjective trust of Swiss voters in a short online survey with 1228 participants, considering the trust practices of vote updating, trial elections, open-source disclosure, verifiability by code sheets, and expert evaluations. The participants were asked how the practices impact their trust and could choose between 1) it increases their trust, 2) it does not increase their trust, or 3) they do not know. Further, Milic *et al.* compared perceptions of online, in-person, and postal voting. The authors found that trust in online voting was generally rated lower compared to in-person and postal voting [46, 61]. However, most survey participants did not report any online voting experience. Those who reported experience rated their subjective trust in postal and online voting similarly. The option to participate in a trial election on a demo website and individual verifiability were identified as practices that could increase the trust of a significant share of participants. This was followed by expert evaluations. About half of the participants stated that not knowing how the source code disclosure would impact their trust. While these data serve as a basis for further investigations, the reason why the specific practices impact voters' trust and whether this might be related to misconceptions remains to be answered. Compared to the work of Milic *et al.*, we investigate a more comprehensive set of practices and collect qualitative data from the participants to gain a deeper understanding of *why* and *how* the specific practice impacts subjective voter trust.

Related work investigated trust in connection to specific online voting systems. Investigations of online voting diffusion in Estonia over a period of ten years showed that trust in online voting overall decreases over time but still is an essential impact factor [68].

2.3.1 Human Factors in Online Voting

Human factors in the scope of online voting schemes have been investigated by related work. Among those are usability studies [2, 24, 35, 36, 40] and user experience studies [17, 41, 43]. Usability studies revealed that mere usability is not enough to convince voters due to the complexity of online voting schemes. For instance, verification mechanisms that are probabilistic, meaning that additional spoiled votes can be verified but not the cast vote, were perceived as unnecessary [40, 43]. Investigations of the Norwegian online voting prototype showed that voters had difficulties determining whether their votes were indeed submitted [24]. On the other hand, voters are willing to sacrifice usability for security because this enhances their trust [11]. Further studies that investigated specific voting schemes showed that information given to voters in the voting software and on informative material could impact subjective trust [41].

3 Trust Practices

In this section, we first detail our literature search and identify trust practices.

3.1 Identifying Trust Practices

A *trust practice* is a task carried out by the voting or independent authorities that is not required as part of the functionality of the core online voting system. Hence, a trust practice goes beyond the minimum required functionality of a voting system and offers additional information for voters. To collect state-of-the-art practices for our investigation, we conducted a structured literature search [72, 74] and an online search. In the first step, we searched paper abstracts in scientific databases based on *keywords* to create an initial list of papers. As keywords, we used combinations of *trust* AND (*measure** OR *practice**) AND (*e-voting* OR *electronic voting* OR *Internet voting* OR *online voting*). We searched the scientific databases ACM, IEEExplore, and SpringerLink and the proceedings of the venues[1] that publish e-voting related papers. Those are

[1]The searched conferences were the International Conferences on Electronic Voting (EVote), Electronic Government (EGov), Electronic Partici-

Table 1: Overview of trust practices extracted from related work. Some references in the list of countries refer to scientific papers.

Trust Practice	Sources (Literature)	Sources (Countries)
Expert Evaluations	[46,48,67,71]	Switzerland [56], Estonia [19], Norway (Trial) [71]
Individual Verifiability	[46,48,67,71]	Switzerland [56], Estonia [19], Norway (Trial) [71], Australia [30], New Zealand (Trial) [18]
Vote Updating	[46,67,71]	Estonia [19], Norway (Trial) [71]
Open Source Disclosure	[46,48]	Estonia [19], Switzerland [56]
Trial Elections	[46,67,71]	Norway (Trial) [50], Switzerland [56], New Zealand (Trial) [18], Lithuania (Trial) [9]
Independent Implementations	[35,36,71]	-
Media Information Campaigns	[48,71]	Norway (Trial) [71], Estonia [20], Switzerland [56]
Support Service for Voters	-	Switzerland [56]
eID Authentication	[51]	Estonia [19]

related to electronic voting but not published in the mentioned databases.In this step, we identified 267 papers. We excluded papers that just mentioned the keywords without a connection to our research topic, e.g., publications focusing on computational trust. This drastically shrunk the list of relevant papers since most existing research is related to computational trust or subjective trust into specific voting systems or interfaces.

Based on the initial list of papers (N=6), we performed a forward and backward search based on Google Scholar, identifying one additional paper [46]. Publications found during this phase could be published in any database. Besides the scientific literature, we consulted publicly available information about existing online voting systems from different countries and organizations based on the list of countries with online voting or online voting trails offered by Verified Voting [69]. The literature search was conducted in early 2020; hence publications were published until then.

That resulted in seven scientific papers and seven online resources that specifically detailed trust practices (see Table 1). To cluster the practices, two researchers independently extracted a practice list from each paper and resource by copying the text describing the practice. After comparing and discussing the created lists, the researchers followed an inductive categorization approach to categorize practices until further categorization is no longer meaningful. Finally, for each practice category, an identifier (e.g., "expert evaluations") and description were created in cooperation. This resulted in nine categories of state-of-the-art practices (see Table 1).

3.2 State-of-the-Art Practices

In this section, we detail the practices obtained from the literature. Those practices were investigated in our study.

Expert Evaluations. As first practice, we identified expert evaluations that refer to an inspection of the implementation of the online voting scheme and all corresponding components. Expert evaluations can be based on international standards, such as the Common Criteria for Information Technology Security Evaluation [14]. There are several realization possibilities: authorities could assign specific institutions to conduct an evaluation or run penetration tests. Furthermore, the source code can be made available to any expert interested in it. For example, Switzerland [25, 29], Estonia [31, 32] and Norway [26] based their Internet voting systems on voting protocols that have been published in international peer-reviewed conferences. Several security properties of these voting protocols are formally proven with mathematical methods by experts or have been reviewed. For instance, Norway's mechanism for individual verifiability has been analyzed and discussed by experts [6]. Switzerland has performed a public penetration test in 2019 [15]. Therefore, they made the source code available to the public and offered financial rewards for the reporting of vulnerabilities. As a result, several vulnerabilities were reported.

Individual Verifiability. Individual verifiability means that the voting scheme offers voters means to verify that their votes have been cast as intended. This allows voters to confirm that the vote registered in the electronic ballot box matches their intentions. For instance, Estonia enables individual verifiability by an app on a mobile device [32]. Switzerland uses schemes based on verification codes [25]. Norway used a similar scheme for their trial Internet elections [26]. There are several Internet voting protocols that enable end-to-end verifiability. This allows voters to confirm that their vote is included in the final result. Such protocols have been deployed in low stake elections, such as the university election in Belgium [4].

Vote Updating. Vote updating enables re-casting and replacing previously cast votes. The reason for this is that voters can re-access the voting software anytime without fearing consequences. This also mitigates vote-buying and voter coercion as votes cast in the presence of a coercer could be re-cast later on [71]. For example, Estonia's i-Vote scheme enables vote updating [19]. Less than 3% of Internet votes were re-cast during the past Estonian elections [21].

Open Source Disclosure. This practice is disclosing the source code of the used voting software with the exception of

pation (EPart), and Usenix Security. The workshops were the Electronic Voting Technology Workshop (EVT) and its successor Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE). Furthermore, the USENIX Journal of Election Technology and Systems (JETS) was searched.

sensitive data such as keys or authentication data. In doing so, any individual or institution could review the source code and report vulnerabilities or bugs. The source code of the system used during the trial elections in Norway is published. This system has been audited by security experts [8]. The Estonian system is published online[2] except for the voting software that the voters use. The source code and other properties of the Estonian system were, for instance, analyzed by an independent research group from the US [66]. As mentioned above, the Swiss Post system is published for public penetration tests, and Swiss Post announced they will publish all subsequent versions of the voting system [56].

Trial Elections. This practice deals with the possibility for voters to become familiar with the Internet voting software before participating in a real election [71]. Considering DOI, it targets the construct of trialability. Further, trial elections can support voters in assessing the compatibility of an online voting system to their values, beliefs, and needs. There are several possibilities to realize this practice. The first is organizing a trial election on a specific date with a fully working system, including support hotlines and the distribution of voting credentials to voters. Norway, for instance, has conducted two trial elections in 2011 and 2013. Lithuania currently plans an Internet voting trial by allowing expats to vote online [9]. The second option is providing a demo voting system. This system can be accessed at any time without the need for extra credentials. For instance, Swiss Post offers such a system and a website with information about their Internet voting system [55].

Independent Implementations. The practice of independent implementations means that the voting software (and verification software) should be available from different institutions [35, 36]. In doing so, the voters can choose a voting software from the institution they trust most or could switch the voting software if they experience problems. However, independent implementations can have further ramifications. Malicious third parties might provide malicious voting software that steals credentials or manipulates votes. Hence, if realized, this practice needs additional effort to prevent malicious voting software. To our knowledge, this practice has not been used in Internet elections yet.

Media Information Campaigns. Media information campaigns aim to offer explanations of the Internet voting scheme. This could be TV spots, informative videos, or online documentation. Voters can access the provided information to inform themselves about the voting procedure before the real election. Thus, they can familiarize themselves with the procedure and security-related information on an individual level. Estonia, for instance, offers a website with detailed information about its i-voting system [20]. Considering the DOI, media campaigns target the construct of observability. Similar to the trial elections, media information campaigns can support voters in considering compatibility.

Support Service for Voters. This practice refers to providing a support team that can answer voters' questions about the Internet voting system. This includes technical inquiries and also assistance for voters during the voting process. Switzerland, for instance, offers a support hotline that voters can call if they require assistance during voting.

eID Authentication. The practice describes an authentication method using an electronic identity card. Previous studies have shown that users of a system evaluate its security based on the authentication mechanism [78]. In Internet voting, authentication is crucial since only eligible voters are allowed to participate in the election. Estonia, for instance, uses the national ID card for checking the eligibility of voters [20].

4 Methodology

To investigate perceptions of nine the state-of-the-art practices, we conducted an interview study with 26 participants. We chose semi-structured interviews because they offer a certain structure while at the same time providing enough freedom to investigate participants' perceptions in depth [49]. Before the study, we conducted two pilots interviews to validate the clarity of our questions. In our investigation, we focused on national elections for parliaments, because these elections have the highest possible stake.

4.1 Interview Procedure

After welcoming the participants and introducing the goal of the study, participants read and signed a consent form. We then followed the hereinafter procedure which took 60 minutes per participant.

1) Experience: We started the interview by asking the participants about previous voting experiences and their opinion and knowledge on electronic and online voting.

2) Familiarization: In this step, we exposed the participants to screenshots of an online voting website and an official-looking electoral letter. The screenshots show the system that was used in Switzerland for online voting but the design is based on recommendations from related work [41]. More specifically, a comparative study of individually verifiable schemes had shown that this particular system offers high usability and user experience while being understandable to voters compared to other classes of individually verifiable schemes [43]. We did not mention that this system was used in real elections, instead we told the participants that

[2] https://github.com/vvk-ehk/ivxv accessed 23-Sep-2021

this is how a possible realization of online voting could be like. The concept of verifiability is online voting is novel and might be challenging to understand in theory [17]. Hence, the familiarization had the purpose to make sure participants understood the concept. After the familiarization, we specifically asked the participants whether they have any questions about the presented voting system and made sure that they understood the concept of individual verifiability.

3) Trust Practices: During this part, we presented the nine state-of-the-art practices (see Section 3.2) for fostering subjective trust in online voting. We iteratively developed presentation slides with descriptions of the practices. The slides were reviewed by HCI experts and tested in trials. The order was chosen to support understanding practices from familiar to more unfamiliar ones. Trial participants gave feedback to improve the order that was initially randomized. For each practice, we asked participants to explain in detail how and why the presented practice impacts their trust. We then asked the participants if any further factors could impact their subjective trust, and if any practices should be added to the list. Finally, we asked the participants to fill in a demographics questionnaire. At the end, we thanked the participants for participation and gave them the opportunity to ask questions.

4.2 Recruitment and Participants

Before conducting the interviews, we carefully discussed a recruitment strategy. Overall, there are several countries that permit online voting for political binding elections. However, for most of them, such as Armenia, Switzerland or Australia, the share of active online voters is extremely low since online voting is only permitted to a specific demographic, mostly voters that are located abroad. Further, voting channels are forming a habit meaning that once someone has used online voting, they are likely to use it again [70] based on learned trust. To avoid an interference of the habit, learned trust as well as the familiarity heuristic [60], we recruited a sample that has never voted online before and who never lived in a country that offered online voting.

We conducted the study with 26 participants (10 female, 16 male) between 19 and 60 years ($M = 27.5$, $SD = 9.4$). All participants were from Germany and had suffrage there. The age group of our sample reflects those most interested in online voting in Germany [27]. Twelve participants had a bachelor degree, seven a high school diploma, five master degrees, and two named middle school as their highest education. Fourteen participants were students of different subjects. Considering occupation, two were environmental carers, two artists, two engineers, one researcher, one teacher, one gardener, one linguist, one system planner, and one developer. Ten of the participants either worked in a technical-related job or studied a technical-related subject at university. All participants were recruited through online social media, announcements on our university's mailing lists, and poster advertisements. The recruitment material mentioned that we look for participants in an interview study about electronic voting. We kept recruiting until saturation was reached by three repetitive answers. After that, we continued with six further interviews.

Except for one participant, all participants were active voters during political elections, such as parliamentary elections (N=22), local elections (N=18), and state elections (N=15). The self-described "convinced non-voter" reported to have assisted as poll worker in a regional political election once. Most of the participants (N=17) are voting using both, on-site ballot box or postal voting, while four only use one of the methods exclusively. Only one participant stated to have voted electronically in a university election.

We further assessed the participants' opinions about online voting in general. Of the 26 participants, N=12 reported to doubt the overall concept and expressed scepticism against it. The remainder expressed a neutral or positive attitude.

4.3 Data Analysis

All interview recordings were transcribed into written form. Next, two researchers familiarized themselves with the transcripts by reading them repeatedly. Since, we build upon the results from Milic *et al.* [46], we decided to follow an deductive approach based on the main research question *How did the proposed measures impact the perceived trust?* Milic *et al.* provided three options to participants for trust assessment: 1) positive, 2) negative and 3) do not know. Based on that, we used *positive impact*, *negative impact* and *neutral impact* as a basis. To make sure that these codes consider the entire answer spectrum, two researchers analyzed two randomly drawn interviews and proposed a separate codebook based on the main research question. In a review meeting, a final codebook was agreed upon. The codes from Milic *et al.* were extended by *mandatory practice*. We furthermore coded *new practices*, *misconceptions*, and explanations that are not related to subjective trust by using the code *no clear option*. For the codebook, readers are referred to Appendix 2. Both coders applied the final codebook to all transcripts independently with an 76% agreement. To determine the interrater reliability, we calculated Cohen's κ, which is 0.676 (substantial agreement [16]). Because Cohen's Kappa was relatively low, the coders discussed all code allocations in a follow-up meeting. The main discrepancy was related to the code *misconception*. In the review meeting, the coders agreed on final unambiguous allocations. After coding, we clustered the practices into groups of mandatory, positive, neutral and negative practices based on the share of participants by majority of code allocations meaning at least half of participants gave a statement coded with a specific code or the a specific direction could not be determined resulting in a neutral practice.

4.4 Limitations

Like most qualitative and exploratory work, our study holds several limitations. Interviews rely on self-reported data, hence they might be subject to the social desirability bias, availability bias, and wrong self-assessments. Due to the qualitative nature of our study, quantitative conclusions cannot be drawn. Although our sample reflects those who are interested to participate in online elections in Germany [27], it might not be representative for the overall voter population. In the last federal election in Germany, 36% of voters were over 60 years old [54]. This age group is underrepresented in our study. Further, the results are limited to German voters. Previous studies showed that voter experience with a voting technology can impact study results [42]. To address this, we made sure that our participants have a consistent voting experience, namely they have not participated in political online elections before. Consequently, our results do not consider voters with online voting experience. The order of the practices was determined using pilot interviews in order to provide a logical order. This might have disadvantaged practices that were presented towards the end due to sequential effects. However, the benefits of following a logical order outweighs the disadvantages of sequential effects because our pilot tests showed that a specific order supports the participants' understanding of the specific practices. Finally, the practices were given to participants in textual form in a rather generic level. We opted not to include specific organizations and institutions since those might impact the participants' trust. Consequently, our investigation should be seen a a first step of investigating trust practices which should be continued by investigating more specific realizations with a more diverse sample in different countries.

4.5 Ethical Considerations

While there is no formal institutional review board process in our institution, our study complied with our institution's ethics regulations and national privacy regulations. Before analysis all interviews are transcripted into written form. The interviews were conducted online through a video calling software that was hosted by the author's institution. Collected data was stored in an encrypted cloud hosted at our institution. Only the authors had access. Participants were allowed to abort the study any time without fearing negative consequences, skip questions, and were informed about data handling. No identifying information besides name and signature on the consent form was collected.

5 Findings

Based on the answers given by our participants four types of practices could be determined: 1) *mandatory*, 2) *positive*, 3) *negative*, and 4) *neutral*. This refers to the impact of the specific practice to the participant's subjective trust. Additionally to that, participants expressed several *misconceptions* that impact their trust.

5.1 Mandatory Practices

Several practices were considered mandatory by the participants. This means that the specific practice is considered a prerequisite for participating in online elections in general. In particular, *expert evaluations* and *media information campaigns* were considered to be mandatory.

Expert Evaluations: Most participants (N=22) stated an evaluation by experts is a must-have for them. For instance, **P03** stated: *"I consider it as essential that someone independent is involved and not a private company who is setting up the whole thing and then passing on votes [to a third party]."* and **P24** said: *"As a matter of course, it should be checked by experts."*

Furthermore, ten participants commented on the independence of the experts and stated that it is important for them. **P15** mentioned: *"If there are reasonably independent experts, to most people, it will be an objective assessment. This conveys security."* while **P01** said: *"The term experts always sounds great. On the other hand, how can I be certain that these experts are really independent?"*

Some limitations of expert evaluations were also mentioned. For instance, experts might be influenced by a malicious third party (N=5), or their credibility might be questioned (N=4), e.g., **P12** said that *"experts still can be influenced. This is not equivalent to voluntary election assistants."* **P21** mentioned that *"I do not know who these experts are. Why is anyone an expert? I don't always trust someone just because they claim to be an expert."*

Media Information Campaigns: Media information campaign (N=17) and publicly available information about online voting form the next mandatory practices (N=17). Several participants mentioned that this practice to be a prerequisite for them, such as **P06:** *"I also see this as a prerequisite. Before this [the election], it has to be explained to people how it works. And it must also include how they evaluate my data – in a way that is understandable for regular citizens."*or **P20:** *"A prerequisite for me. Especially if online voting is new and it is taught to people in a reasonable manner. Technical details would also be beneficial for interested people. If such things did not exist, I would be very skeptical."*

Two participants particularly mentioned that TV spots should be broadcast after election commercials. The first one was **P24:** *"This could be tied to the election commercials. Not everyone is on the Internet - but older people in particular watch TV, and they see it. This would be a good approach."* The second one was **P18:** *"Would be a good addition to election advertising."*

5.2 Positive Practices

In this section, we detail the practices that our participants perceived as positive. Those are *individual verifiability*, *trial elections*, and *support for voters*.

Trial Elections: Trial elections were also deemed positive. Most participants (N=19) indicated trial elections would improve their subjective trust. Participants, especially those with less technical knowledge, appreciated the opportunity to experience and learn the process in a neutral environment before the election. Participants also mentioned that this practice improves trust because it leads to voters making fewer errors which in turn leads to more votes being cast as intended. **P02** stated: *"I like it. Because then you have done it before. If it is more familiar, then you trust it more."* Another representative example is from **P08:** *"I think that's a good idea. Especially for people who are not that technology or Internet-savvy. They could familiarize themselves with it [names example]. It would also increase my trust in the final result since I believe there would be more actual intended votes."*

Only one participant stated a negative view and two participants a neutral view towards trial elections. In contrast, four participants provided an answer with no clear opinion towards their subjective trust. The negative view stated that voting systems should be intuitive enough, such that familiarization, which would come with additional effort, is unnecessary. The neutral positions were that a trial election is maybe useful for other people but not for themselves since they are capable of understanding it without a trial, such as **P03:** *"I think it's stupid. If I got something like that, I would think that I have to practice. It [the voting software] should rather be as intuitive as possible."* or **P19:** *"I do not think that this is absolutely necessary. For me, it is obvious how it works. Maybe it is useful for other people."* When we told participants about trial elections, two participants mentioned to consider them important to start with local elections or polls, **P13** stated: *"Start off small as a trial, for instance for local referendums, to see if the system works and cannot be manipulated. Something like this might be good."*

Support Service for Voters: The practice "support service for voters" was deemed positive by most participants (N=16). They saw support services as a positive feature that improves their subjective trust.

Within this practice, our participants considered it a positive practice because they personally would like to use such a service and hence consider it as a personal benefit. One even considered it a mandatory practice for an information campaign. **P08** reported: *"In general, whenever any kind of assistance is offered, you might be more open-minded towards the topic. If something really happens, you would know who to contact."* and **P10** mentioned *"The possibility to get answers directly increases my confidence in the system."*

Only one participant was negative towards this practice, while five remained neutral, and three stated no clear opinion towards their subjective trust. The negative participant feared the possibility of influencing the help-seeking people with this service, while some of the participants with neutral opinions about this practice did not believe in the usefulness and effectiveness of such this measure. Others stated they do not need such service and hence it does not increase their subjective trust, but still consider it important for other voters, such as **P01:** *"So like a hotline? I think it's difficult. On the one hand, it makes sense to be able to ask someone if you don't understand something. On the other hand, the risk is if an elderly confused grandmother calls and is manipulated by the person on the phone."*

One participant (**P16**) stated that it could be implemented not only as a hotline or help desk but (additionally) as an online resource providing video material with details about the technical backgrounds of the voting: *"I could imagine that there is a YouTube channel that explains the technical background in more detail."*

Individual Verifiability: The practice of individual verifiability was generally deemed positive. Most participants (N=12) provided responses indicating that vote verification increases their trust towards voting systems. In particular, providing feedback to confirm that one's vote has actually been registered in the electronic ballot box was viewed as positive and as a form of improved control, e.g., **P04** said: *"The feedback alone is mentally quite good for the personal feeling."* and **P05** mentioned *"Had the feeling that I had some control over the integrity of my data."*

Only two participants stated a negative or a neutral view towards verifiability, respectively, while ten participants answered without a clear opinion. Too much complexity and a lack of faith in the system's effectiveness prevented an improvement in the subjective trust of these participants. The possibility that attackers could still fake verification data was also mentioned, like **P21:** *"It [the vote] can still be faked if an attacker can reproduce the codes."*

5.3 Negative Practices

Several practices would impact the participants' trust negatively. Namely, those are possibilities for *vote updating* (N=15) and *independent implementations* (N=23) of the voting software.

Independent Implementations: Independent implementations were considered a negative practice by most participants.In addition to their concerns about additional security issues due to the several implementations, participants feared fake apps that could try to manipulate their votes. They were also concerned about the influencing effects of different user interface designs, such as colors. They also thought that meta-

information about the app, such as the number of downloads or the app developers, could influence their decision to use it. A sample comment is given by **P03:** *"I think it's important that there is one app that is not made by some weird company but by the government. Users could be manipulated through the user interface. I also find it very dubious if companies would want to publish their own election app."* and **P16:** *"While it's nice if everyone can do their own thing, it would negatively affect my trust in integrity. That would possibly lead to political parties writing their own apps. The number of downloaded apps would give a pre-election result and, thus, influences the citizens before voting."*

Only one participant was positive or neutral, respectively. One stated no clear opinion towards subjective trust. While the positive participant acknowledged the additional attack vector through multiple implementations, they also stated not having to trust a single entity outweighs the aforementioned drawback in their view. The participant (**P20**) that was neutral about this practice did not find it useful or necessary *"This creates an additional attack vector through manipulated front-end websites with directed disinformation campaigns. However, it gives you more certainty because you are not forced to trust the election officer."*

Vote Updating: The practice of vote updating was evaluated as negative with respect to the subjective trust by most participants (N=15). Raised concerns were the possibility of counting not just the last vote, thus compromising the final result, the greater risk of being manipulated and changing own vote accordingly as well as the opportunity for third parties to change the vote after casting. Additionally, participants stated that online voting should be the same as paper-based voting, and therefore no vote updating should be possible.

In addition, participants expressed that voters should make up their minds before rather than during the elections. Sample comments are: **P02:** *"Difficult. I don't think it's so good that you can change it [the vote]. Before you vote, you should inform yourself, and then I think the vote should be final. Manipulating the environment can otherwise take place much stronger."* or **P11:** *"I have the feeling that it is becoming more insecure. Maybe there is another way to manipulate this additional process."* and **P20:** *"When you vote, you should vote and not change your mind five times. One should deal with it [decision making] before."*

Only two participants were positive, while seven remained neutral, and two stated no clear opinion towards this practice's impact on their subjective trust. It was seen as positive that people's opinions can change and that this should be taken into account in the voting system. Although vote updating does not protect against influence by third parties completely, it allows coerced voters to update their votes once the coercer is no longer present. Those who were neutral expressed that they had little experience with the mechanism or did not want an option to update their vote, such as **P17:** *"Many people might change their mind, and I find it useful to be able to change my vote."*

5.4 Neutral Practices

The final group of practices are those that our participants considered not to impact their subjective trust perceptions. Such practices were either considered as nice-to-have or as something without a direct benefit for the participants. Neutral practices are *open source disclosure* and *eID authentication*.

Open Source Disclosure: This practice was diversely perceived as seven participants stated a neutral view, because they do not bother, are not able to read source code, or assume the vast majority of the people cannot read source code, such as **P10:** *"I would not look at the code and can't do anything with it."* or **P22:** *"Seems a bit hypocritical because 99.9 percent can't read that at all. So it would rather be a pseudo measure. On the other hand: People could also see that something is being done. This could then contributes to the establishment of trust. So it could be one way or another."*

Ten participants positively perceived the practice because they saw the opportunity that even more audits could be done when the code is open source. They also assumed that the code has to be of high quality if it is published, which would positively influence their subjective trust, for instance, **P03** said *"I do not have a strong opinion on this. I just find it great, as it suggests that the software is already pretty good. I also believe that people who are smart enough would find the vulnerabilities."* or **P05**'s comment *"Because then I can verify it - anyone can verify it. Even the malicious, but hopefully we have more good than bad people."*

In total, five participants had a negative view towards open source disclosures, primarily because they assumed this practice makes it easier for criminals to find vulnerabilities and compromise the vote in their favor, e.g., **P04:** *"People who want to harm you can find vulnerabilities much easier. Which is why I would be rather against it. If the independent experts from before have already assessed it, then I would find it much better. Yet there are always nerds who want to prove that they can attack something."* or **P19:** *"I think this is absolutely bad. If the code is open and can be seen by everyone, it would be vulnerable to certain groups. This could potentially be used to fake the election."*

Last but not least, one participant (**P20**) saw it as a mandatory practice: *"In my opinion, this is a prerequisite for me to support the electoral system. If that were not the case, I would protest against it."*
In sum, four participants provided an answer not concerning their subjective trust towards a voting scheme.

eID Authentication: Four participants stated a neutral view, primarily because they see no additional benefit in using the

eID compared to a password or code sent by postal mail. **P01** mentioned that *"It is definitely beneficial to identify yourself with it, but I considered the login code already as sufficient. I don't think anyone would take all the effort to distribute fake credentials to the electorate."* while **P05** said *"Physical tokens can also be faked. Thus, there is no difference between that and credentials."*

Twelve participants had a positive position towards the practice because they assumed it is a secure technology since it is a legal document. It is also widespread, and nearly everyone owns one. Another argument was that the eID cannot be stolen by the mailman, for example, or guessed by a hacker like a password. **P07** commented *"Because I would rely on a proven technology that I know from everyday life and use for identification. You know it, but maybe not everyone has it."* and **P11** said *"To me it suggests more security, because the ID is an official document."*

In total, eight participants had a negative view towards this practice, primarily because they were concerned about the privacy of their vote and whether they could be identified if they used eID. Another reported hurdle could be the need of an additional device to read the eID which everyone would need. We discuss this further in Section 5.5. One participant (**P06**) also saw it as a mandatory practice to establish trust in the first place, although they could not assess whether it would be secure and whether identifying them would be possible: *"Is necessary for me. Yet I can't judge whether the security behind it is good enough. I certainly don't want to have my vote associated with me afterward."* Only one participant reported that eID Authentication does not impact their trust.

5.5 Misconceptions

When explaining the impact of the practices on their subjective trust, the participants mentioned several aspects that we identified as misconceptions.

Vote Privacy Breaches: In connection with eID authentication and individual verifiability, eight participants thought that these features could potentially threaten their vote privacy. However, vote privacy is preserved by state-of-the-art verifiability protocols, e.g., [25], yet verifiability features are frequently mistakenly interpreted to violate vote privacy, see e.g., [80]. In the scope of eID authentication, eight participants particularly feared that the vote might somehow be linkable to their identities, such as **P03:** *"I see a greater risk that my vote could be linked back to me. With the codes, I have the feeling that they were randomly generated by some algorithm."* and **P04:** *"I would rather have only a password and no ID card. Otherwise, I would have the feeling that it would be easier to trace back to me."*

Two participants thought that the codes used for verification might be linkable to their identities by the authorities, e.g., **P06**: *"I like it, but for this to work, they must have saved my data somewhere. With this, you can make a connection between me and my vote again. I think this is stupid."*

Impact of Open Source Disclosure: Open Source disclosure was, on average, perceived as a neutral practice. This perception might be related to the participants' impression that the disclosure of source code could impact the security of the voting system negatively.

Nine participants stated that adversaries might use the published source code to find vulnerabilities leading to an increased chance that the system might be hacked, e.g., **P02:** *"Criminals can also find weaknesses. I think it's enough to explain how the system works."* and **P13:** *"Through these publications, people who can manipulate something can also discover vulnerabilities more easily."*

5.6 New Practices

At the end of the interview, we asked the participants about further practices they consider important in the scope of online elections.

Role Models and Social Media: Several participants mentioned that role models, such as politicians, would have an impact on their subjective trust. In particular, if politicians would recommend online voting and use it, the trust from participants is positively impacted. For instance, **P03** commented *"Politicians, for example, are a symbol for the entire population; therefore they should begin with it. I would set everything into a larger context. For example, embedding it in the political landscape 'that we are saving trees now'. That would also create trust."* while **P24** said *"For example, if the Minister of the Interior were to say that this is safe, I would trust the whole thing."*

While this is not a practice that can be ordered from the authorities, participants in our study particularly wished that participation in the online election could be shared through social media by anyone. Two participants stated that the voting software should encourage voters to do that by integrating social media share buttons, such as **P10**: *"A possibility is to share the participation in the election, e.g., in social media, to share the trust on behalf of others."*

Secure Hardware: The final new practice is related to security. Participants wished to receive a special hardware device that is secure and exclusively used for voting. **P05** mentioned a USB stick: *"A more detailed overview of the security process is very important for those who are interested. Furthermore, malware on the device is still a problem. With this, you can certainly trace back how I voted. Maybe you could provide people directly with a secure Linux (on a USB stick) or provide instructions for it. Smartphones are basically more contaminated."* while **P11** was less specific: *"Free or inexpensive, secure hardware for the population to vote."*

6 Discussion

In this section, we discuss the findings of our interview study. Further, in this discussion, we contribute recommendations to support developers, researchers, and policymakers when designing and implementing future online voting systems.

6.1 Realization of Practices

In this section, we discuss the participants' subjective evaluation of the practices in the context of existing related work and established theories and provide recommendations for trust practices in online elections.

Mandatory Practices are Well-Known from other Domains: Expert evaluations and media information campaigns were considered as mandatory when introducing and offering online voting confirming results from Switzerland [46]. The positive assessment of expert evaluations might be because people are generally used to expert evaluations in other domains, such as car inspections, food control, or e-commerce. Further, several tasks in daily life cannot be fulfilled without trust in experts that check conditions in which laymen's knowledge does not suffice [33,38]. The perceptions of expert evaluations might also be explained by the two-step flow of communication model by Lazarsfeld *et al.* [39]. The model considers individuals to form their opinions based on opinion leaders who could be recognized experts.

People furthermore know media information campaigns from their daily lives. Here, the two-step flow of communication model could be considered as well if opinion leaders are part of media information campaigns. Both practices assist voters in gaining information about online voting. In doing so, they can assess relative advantage and compatibility of the new voting channel, which are DOI dimensions.

In summary, we consider expert evaluations and media information campaigns essential for online voting and also encourage independent evaluations from researchers (cf. [30, 64–66]). *Policymakers and voting authorities are recommended to use practices that are well-known from other domains, such as media information campaigns or expert evaluations*.

Positive Practices: Individual verifiability, trial elections, and support services for voters were perceived as positive trust practices. While trial elections and support services are also well-known from other domains, individual verifiability was a new concept to most participants. Its positive trust impact might be related to transparency. Compared to paper voting, where voters physically interact with their votes, online voting makes it difficult for voters to judge vote processing [43]. Using a verification mechanism, voters can ensure that their votes are registered in the electronic ballot box, matching their voting intention. Earlier investigations of verifiable online voting showed that voters prefer verifiable schemes and would even sacrifice ease of use [11]. However, not all participants stated that individual verifiability would enhance their trust; two participants even feared that it could impact vote's privacy. Related work has investigated specific verifiable online voting schemes and also observed these perceptions [17,79,80] while other investigations showed that vote privacy perceptions are not an issue (cf. [41]). A comprehensive investigation of individual verifiability revealed that the choice of the verification protocol could impact trust [43]. Hence, providing an individually verifiable voting system is not enough because the choice of the specific verification mechanism and the communicated information are crucial. Trial elections allow voters to gain information to assess the complexity of the online voting system and compatibility according to the DOI [59]. It further offers a way to try out a new voting channel without fearing negative consequences, which refers to the trialability dimension of the DOI.

In summary, we recommend online voting systems should offer individual verifiability. Trial elections are also recommended because they offer means to review the voting systems without consequences. Ideally, authorities should perform trial elections before introducing online voting as new vote casting and offer a demo system of the voting software anytime before, during, and after the election.

Realizing Neutral Practices: Open-source disclosure was perceived as neutral practice overall. However, the opinions of individual voters were quite extreme. On the one hand, participants were convinced that this practice enhances their trust. One participant would even abstain from online voting without disclosure of the source code. On the other hand, several participants feared that the security of the voting system might suffer from open-source disclosure which is in line with previous work on secure communication tools [1]. While it is true that adversaries can indeed inspect the published source code to find vulnerabilities, independent experts and everyone interested can also do that.

We argue that simply publishing the source code has a high potential for misperceiving the practice. *Instead, we recommend combining disclosure with a penetration test as done in Switzerland [15]*. In doing so, trust gained from expert evaluations is leveraged to address the misconceptions. Voters perceiving the disclosure as an enhancement are not negatively impacted by the penetration test.

The next neutral practice is eID authentication. Similar to open-source disclosure, two main opinions were expressed. First, it was considered to enhance security since eID authentication is more difficult to fake compared to passwords that are distributed via postal mail. Second, violation of vote privacy was feared, which would introduce disadvantages compared to polling station voting. Whether this is indeed true depends on the specific protocol used for voting and the compliance by voting authorities. Estonia, for instance, uses digital sig-

natures produced by the eID for eligibility checks [32]. For this, digital votes are signed after encryption. To keep vote privacy, the digital signatures are removed from the digital votes before counting. Compliance to this process is observed by experts.

Consequently, we recommend that if eID authentication is deployed, information about the voting system should contain information on how vote privacy is preserved in easy language. This information should be depicted during voting in the voting interface and within the media information campaigns, such that voters can gain information without accessing the voting software. Misconceptions about vote privacy constitute a severe issue because democratic principles are violated. Still, investigations of online voting protocols showed that voters are not always convinced by vote privacy features [17, 79, 80]. As a consequence, communication and voter education alone is likely not enough. *Hence, voter perceptions of vote privacy have to be considered already when choosing the voting protocol.*

Dealing with Negative Practices: Vote updating was perceived negatively, as demonstrated in past surveys [46]. Yet, past surveys and our study were conducted in countries where updating of paper votes is not possible. Estonia allows updating online votes; however, this feature is barely used by voters [21]. When participants were confronted with reasons for vote updating, they were not convinced that vote-buying and coercion are indeed mitigated which is true because coercers might act last-minute, such that voters have no chance of updating their votes. Because of that, *these features should be communicated with care without making unrealistic claims*. Further, trust is likely decreased when additional features do not match the voters' mental model of voting [40, 43]. Based on this negative perception, *we recommend that online elections should closely follow the rules from paper elections and thus not allow re-casting of votes and and then gradually introduce new features that extend the rules from paper voting.*. Within the scope of independent implementations, voters feared fake voting software. The distribution of fake voting websites has already been demonstrated for Switzerland's online voting scheme and is a serious issue. However, the attack was not used in real elections and thus demonstrated the feasibility. We, therefore, argue allowing a limited number of official implementations from officially listed institutions and sources and providing voters with information.

Suggested New Practices: Sharing election participation on social media was considered a practice that impacts trust. By sharing, voters could see that others use online voting. Since the implementation of share buttons can impact website privacy, it should be realized in a way that social media providers do not get any information without the consent of voters. Furthermore, if realized, integration of social media should be discreet to avoid discouraging privacy-aware voters. Role models that publicly express to vote online were also considered as a new practice. This is directly related to the two-step flow of communication model by Lazarsfeld *et al.* [39] mentioned above. Here, the role models can be considered opinion leaders. The second new practice was secure hardware. In particular, participants wished to receive a device dedicated exclusively for voting with software that is tested extensively. This could be realized by trusted hardware tokens with limited computational capabilities and without an Internet connection, for instance, as detailed in [28]. There are several voting protocols that rely on trusted hardware tokens, such as *Du-Vote* [28].

6.2 Impact on System Design

Besides organizational aspects, there are different options to realize the trust practices in the form of systems. In this section, we discuss the impact of our results on system and communication design.

Voting Interface Design: The voting software is used by the voters for vote casting. Based on our discussion of the investigated practices, we consider the following information to be needed during the voting process, such that voters are effectively supported during vote casting. The misconceptions based on vote privacy were quite severe in the context of verifiability and authentication. Hence, voters should receive information that their vote privacy is guaranteed during these tasks. Future work should investigate the degree of information needed to show voters that their votes are indeed private and that their voting choice cannot be linked to their identities. Previous work investigated information placement in voting interfaces and showed that security-related information and detailed instructions are welcomed by voters [41] , but security-related information is often also overlooked [17] showing once more that more investigation on how to communicate with voters is needed.

On the other hand, the voting interfaces are often websites, and voters use their own devices for vote casting. Hence, it cannot be ensured that these devices are malware-free, and malware might even change the appearance of a voting website [41]. Therefore, it is crucial to also place information in other places that we detail below.

Information System Design: Participants in the study welcomed access to information before voting. Hence, there should be different kinds of information systems that (potential) voters can access at any time. One possibility for that are information websites provided by the authorities. Such websites should have different levels of information details, such that voters can fit the information to their level of expertise in order to assess relative advantages and compatibility. For instance, experts should have access to

a full description of the voting protocol and cryptographic procedures, while laymen voters should have access to information that is easy to understand. Furthermore, information websites should offer a demo system of the voting software that can be accessed any time without barriers such as the need to obtain registered credentials. Besides access to information, voters should have access to help from a support team that can answer questions about the voting process and resolves technical issues. Participants welcomed the idea of an interactive system, which could be a chat or hotline that can be called. Based on the importance of vote privacy, such systems should work without the need for voters to disclose their voting intentions to anyone.

Auxiliary Materials: Before elections, voters are typically notified about the upcoming election via postal mail. This notification could entail further materials and information about the voting system. From a security perspective, postal mail is a channel different from the Internet, and therefore, it is more difficult for an adversary to manipulate both channels.

Communication Alone is Not Enough: So far, the discussed impact on system design was limited to information interfaces. However, participants in our study were uncertain whether verification codes might be linkable to their identity. As stated above, to indeed foster trust, it is necessary to start a voter-centered process as early as possible ideally, the voting protocols are chosen in a way that they are intuitively understood without the need to educate voters. Information communication, trust practices, and secure systems are needed but will not have any impact if the chosen protocols are too difficult to understand and do not convince voters about basic democratic principles, such as vote privacy.

6.3 Future Work

In this section, we identify several aspects that should be investigated further by future work.

First and foremost, in this work, we assumed that authorities might offer a secure system that follows democratic standards. Future work should investigate voter perceptions of the different security aspects of online voting in detail. In particular, the security of the system itself, but also the perception of coercion, vote-buying as well as targeted attacks against election infrastructure should be investigated.

Participants in our study and in studies reported by related work feared that online voting might break vote privacy. While this is possible, in general, cryptographic procedures that keep vote privacy are designed and deployed in elections. The communication of vote privacy, therefore, forms an important task of future works. Several studies have already investigated communication within the voting software of specific voting protocols (e.g., [17, 41]). An overall evaluation of information placement, the provided details, and its impact should be investigated further. Within this scope, it is crucial to provide the required information for voters while not overloading them with information.

Online voting is relatively new for most countries. The long-term effects of trust practices are not yet clear. Trust seems to decrease over time [68]. Based on that, studies should focus on countries in which online voting is used for a longer period of time. Furthermore, if countries introduce online voting as a new vote casting channel, trust practices should be carefully observed, and it should be investigated whether their impact changes over time. Within our study, we presented the practices to the participants, however, they have not interacted with them. Furthermore, the practices were quite generic since we did not want a bias due to subjective trust in specific authorities. Because of that, the impact of trust practices on real elections forms a crucial task of future work. Another direction for future work is to study whether some of the investigated practices could increase trust in and thereby amplify the effect of other trust practices. For example, expert evaluations and media information campaigns could also be implemented to increase trust in neutral practices, such as open-source disclosure or eID authentication.

7 Conclusion

In this paper, we investigated nine state-of-the-start measures for fostering trust in online voting through semi-structured interviews with 26 participants. Our results show that trust practices well-known from other domains are perceived as mandatory. Trust practices that participants might consider optional, such as support service for voters, are still perceived to have a positive impact on subjective trust. Practices that divert from known paper voting procedures, such as vote updating, have a rather negative impact. Similarly, practices that might impact security are perceived as negative. Practices that, on average, were perceived as neutral were based on extreme opinions; participants either voiced a positive impact or were concerned about security. This was the case for the disclosure of the source code. Based on our findings, we discuss the realization of specific practices and interfaces for the communication with voters. We conclude by contributing six final recommendations for realizing the measures and provide guidance for future studies.

Acknowledgments

This work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, grant number 251805230/GRK 2050) and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *Proc. of the IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.

[2] Claudia Z. Acemyan, Philip Kortum, Michael D. Byrne, and Dan S. Wallach. Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems*, 2(3):26–56, 2014.

[3] Ben Adida. Helios: Web-based Open-Audit Voting. In *Proc. of the USENIX Security Symposium (USENIX Security)*, pages 335–348, Berkeley, CA, USA, 2008. USENIX Association.

[4] Ben Adida, Olivier De Marneffe, Olivier Pereira, Jean-Jacques Quisquater, et al. Electing a University President using Open-Audit Voting: Analysis of Real-World use of Helios. In *Proc. of the Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, Berkeley, CA, USA, 2009. USENIX Association.

[5] Hayat Ali and Hanan Al Mubarak. E-voting: An investigation of factors that affect public trust in kingdom of bahrain. *International Journal of Electronic Government Research (IJEGR)*, 14(2):12–27, 2018.

[6] Jordi Barrat, Michel Chevalier, Ben Goldsmith, David Jandura, John Turner, and Rakesh Sharma. Internet voting and individual verifiability: the norwegian return codes. In *Proc. of the 5th International Conference on Electronic Voting (EVOTE)*. Gesellschaft für Informatik e.V., 2012.

[7] France Bélanger and Lemuria Carter. Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2):165–176, 2008.

[8] Tor E. Bjørstad. Source code audit of norwegian electronic voting system. Technical report, 2013. [accessed: 02-Sep-2020].

[9] BNS. Lithuanian government backs online voting, but with caveats. https://www.lrt.lt/en/news-in-english/19/1190786/lithuanian-government-backs-online-voting-but-with-caveats, 2020. [accessed: 09-Sep-2020].

[10] Andrew Brien. Professional ethics and the culture of trust. *Journal of Business Ethics*, 17(4):391–409, 1998.

[11] Jurlind Budurushi, Melanie Volkamer, Oksana Kulyk, and Stephan Neumann. Nothing comes for free: How much usability can you sacrifice for security? *IEEE Security & Privacy Special Issue on Electronic Voting*, 2017.

[12] Lemuria Carter and France Bélanger. The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, 15(1):5–25, 2005.

[13] Lemuria Carter and Ronald Campbell. The impact of trust and relative advantage on internet voting diffusion. *Journal of theoretical and applied electronic commerce research*, 6(3):28–42, 2011.

[14] CCRA. Common criteria for information technology security evaluation. https://www.commoncriteriaportal.org/, 2017. [accessed: 02-Sep-2021].

[15] Catalin Cimpanu. Swiss government invites hackers to pen-test its e-voting system. https://www.zdnet.com/article/swiss-government-invites-hackers-to-pen-test-its-e-voting-system/, 2019. [accessed: 02-Sep-2021].

[16] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1):37–46, 1960.

[17] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. Security - visible, yet unseen? In *Proc. of the CHI Conference on Human Factors in Computing Systems*, pages 605:1–605:13, New York, NY, USA, 2019. ACM.

[18] Electoral Commission New Zealand . Electoral commission new zealand website. https://www.vote.nz/, 2020. [accessed 11-Oct-2021].

[19] Estonian National Electoral Committee. E-voting system general overview. https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf, 2017. [accessed 11-Oct-2021].

[20] Estonian National Electoral Committee. E-hääletamise tutvustus. https://www.valimised.ee/et/e-haaletamine/e-haaletamisest-lahemalt/e-haaletamise-tutvustus, 2019. [accessed 11-Oct-2021].

[21] Estonian National Electoral Committee. Statistics about internet voting in estonia. https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia, 2019. [accessed 11-Oct-2021].

[22] International Institute for Democracy and Electoral Assistance. Icts in elections database. https://www.id

ea.int/data-tools/data/icts-elections, 2015. [accessed: 12-Oct-2021].

[23] Batya Friedman, Peter H. Khan Jr, and Daniel C. Howe. Trust online. *Communications of the ACM*, 43(12):34–40, 2000.

[24] Kristin Skeide Fuglerud and Till Halbach Røssvoll. An evaluation of web-based voting usability and accessibility. *Universal Access in the Information Society*, 11(4):359–373, 2012.

[25] D. Galindo, S. Guasch, and J. Puiggalí. 2015 Neuchâtel's cast-as-intended verification mechanism. In *Proc. of the International Conference on E-Voting and Identity (VoteID)*, pages 3–18, Cham, Switzerland, 2015. Springer.

[26] Kristian Gjøsteen. The Norwegian internet voting protocol. In *Proc. of the International Conference on E-Voting and Identity (VoteID)*, pages 1–18, Cham, Switzerland, 2011. Springer.

[27] Kaspersky Labs GmbH. Stimmabgabe per klick - so steht deutschland zum thema online-wahl. http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky-Studie_Stimmabgabe_per_Klick.pdf, 2017. [accessed: 13-Sep-2021].

[28] G. S. Grewal, M. D. Ryan, L. Chen, and M. R. Clarkson. Du-Vote: Remote electronic voting with untrusted computers. In *Proc. of the 28th Computer Security Foundations Symposium (CSF)*, pages 155–169, Piscataway, NJ, USA, 2015. IEEE.

[29] Rolf Haenni, Reto E. Koenig, and Eric Dubuis. Cast-as-intended verification in electronic elections based on oblivious transfer. In *Proc. of the International Joint Conference on Electronic Voting (E-Vote-ID)*, pages 73–91, Cham, Switzerland, 2016. Springer.

[30] J. Alex Halderman and Vanessa Teague. The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In *Proc. of the International Conference on E-Voting and Identity (VoteID)*, pages 35–53, Cham, Switzerland, 2015. Springer.

[31] Sven Heiberg, Tarvi Martens, Priit Vinkel, and Jan Willemson. Improving the verifiability of the estonian internet voting scheme. In *Proc. of the International Joint Conference on Electronic Voting (E-Vote-ID)*, pages 92–107, Cham, Switzerland, 2016. Springer.

[32] Sven Heiberg and Jan Willemson. Verifiable internet voting in Estonia. In *Proc. of the 6th International Conference on Electronic Voting, Verifying the Vote (EVOTE)*, pages 1–8, Piscataway, NJ, USA, 2014. IEEE.

[33] Friederike Hendriks, Dorothe Kienhues, and Rainer Bromme. Measuring laypeople's trust in experts in a digital age: The muenster epistemic trustworthiness inventory (meti). *PloS one*, 10(10):e0139309, 2015.

[34] Jason Hong. The state of phishing attacks. *Commun. ACM*, 55(1):74–81, January 2012.

[35] Fatih Karayumak, Michaela Kauer, M. Maina Olembo, Tobias Volk, and Melanie Volkamer. User study of the improved Helios voting system interfaces. In *Proc. of the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 37–44, Piscataway, NJ, USA, 2011. IEEE.

[36] Fatih Karayumak, Maina M. Olembo, Michaela Kauer, and Melanie Volkamer. Usability analysis of Helios - an open source verifiable remote electronic voting system. In *Proc. of the Conference on Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE)*, Berkeley, CA, USA, 2011. USENIX Association.

[37] Maxat Kassen. Politicization of e-voting rejection: Reflections from kazakhstan. *Transforming Government: People, Process and Policy*, 2020.

[38] Frank C. Keil. The feasibility of folk science. *Cognitive science*, 34(5):826–862, 2010.

[39] Paul F Lazarsfeld, Bernard Berelson, and Hazel Gaudet. *The people's choice*. Columbia University Press, 1968.

[40] Karola Marky, Oksana Kulyk, Karen Renaud, and Melanie Volkamer. What did I really vote for? On the usability of verifiable e-voting schemes. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, pages 176:1–176:13, New York, NY, USA, 2018. ACM.

[41] Karola Marky, Verena Zimmermann, Markus Funk, Jörg Daubert, Kira Bleck, and Max Mühlhäuser. Improving the usability and ux of the swiss internet voting interface. In *Proc. of the CHI Conference on Human Factors in Computing Systems*, page 1–13, New York, NY, USA, 2020. ACM.

[42] Karola Marky, Marie-Laure Zollinger, Markus Funk, Peter Ryan, and Max Mühlhäuser. How to assess the usability metrics of e-voting schemes. In *Proc. of Financial Cryptography and Data Security*, pages 257–271, Cham, Switzerland, 2019. Springer International Publishing.

[43] Karola Marky, Marie-Laure Zollinger, Peter Roenne, Peter Y. A. Ryan, Tim Grube, and Kai Kunze. Investigating usability and user experience of individually verifiable internet voting schemes. *ACM Trans. Comput.-Hum. Interact.*, 28(5), September 2021.

[44] Stephen Marsh and Mark R. Dibben. The role of trust in information science and technology. *Annual Review of Information Science and Technology (ARIST)*, 37:465–98, 2003.

[45] Stephen Marsh and Mark R. Dibben. Trust, untrust, distrust and mistrust–an exploration of the dark (er) side. In *International conference on trust management*, pages 17–33. Springer, 2005.

[46] Thomas Milic, Michele McArdle, and Uwe Serdült. Attitudes of Swiss citizens towards the generalisation of e-voting, 2016.

[47] L. Nestas and K. Hole. Building and maintaining trust in internet voting. *Computer*, 45(5):74–80, May 2012.

[48] Lars Nestas and Kjell Hole. Building and maintaining trust in internet voting. *Computer*, 45(5):74–80, 2012.

[49] Briony J. Oates. *Researching Information Systems and Computing*. Sage, 2005.

[50] Department of Local Government and Modernization Norway. Ikke flere forsøk med stemmegivning over internett. https://www.regjeringen.no/no/aktuelt/Ikke-flere-forsok-med-stemmegivning-over-Internett-/id764300/, 2014. [accessed: 12-Oct-2021].

[51] Oluwafemi Osho, Victor Legbo Yisa, and Olawale Joshua Jebutu. E-voting in nigeria: A survey of voters' perception of security and other trust factors. In *Proc. of the International Conference on Cyberspace (CYBER-Abuja)*, pages 202–211, Piscataway, NJ, USA, 2015. IEEE.

[52] Andrew S. Patrick, Pamela Briggs, and Stephen Marsh. Designing systems that people will trust. *Security and Usability*, 1(1):75–99, 2005.

[53] Wolter Pieters. Acceptance of voting technology: Between confidence and trust. In *Proc. of the International Conference on Trust Management*, pages 283–297, Cham, Switzerland, 2006. Springer.

[54] Demographie Portal. Altersspezifische Wahlbeteiligung. https://www.demografie-portal.de/DE/Fakten/wahlbeteiligung.html, 2021. [accessed: 02-May-2022].

[55] Swiss Post. E-voting. https://evoting.ch/en, 2020. [accessed: 02-Sep-2021].

[56] Swiss Post. Publications and source code. https://www.post.ch/en/business-solutions/e-voting/publications-and-source-code, 2020. [accessed: 02-Sep-2021].

[57] Jordi Puiggalí, Jordi Cucurull, Sandra Guasch, and Robert Krimmer. Verifiability experiences in government online voting systems. pages 248–263, 10 2017.

[58] Brian Randell and Peter Y. A. Ryan. Voting technologies and trust. *IEEE Security & Privacy*, 4(5):50–56, 2006.

[59] Everett M. Rogers. *Diffusion of Innovations*. Simon and Schuster, 2010.

[60] Norbert Schwarz and Leigh Ann Vaughn. *The availability heuristic revisited: Ease of recall and content of recall as distinct sources of information*. Cambridge University Press, 2002.

[61] Uwe Serdült and Victor Kryssanov. Internet voting user rates and trust in switzerland. pages 211–212, 2018.

[62] Fouad Shat and Elias Pimenidis. E-voting versus e-trust: A case study for e-democracy in palestine. In *Proc. of the European Conference on Digital Government*, page 195. Academic Conferences International Limited, 2016.

[63] Elizabeth Sillence, Pam Briggs, Lesley Fishwick, and Peter Harris. *Trust and Mistrust of Online Health Sites*, page 663–670. ACM, New York, NY, USA, 2004.

[64] Michael Specter and J Alex Halderman. Security analysis of the democracy live online voting system. In *30th USENIX Security Symposium (USENIX Security)*, 2021.

[65] Michael A. Specter, James Koppel, and Daniel Weitzner. The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In *29th USENIX Security Symposium (USENIX Security)*, pages 1535–1553, 2020.

[66] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. Security analysis of the estonian internet voting system. In *Proc. of the Conference on Computer and Communications Security (SIGSAC)*, pages 703–715, New York, NY, USA, 2014. ACM.

[67] Oliver Spycher, Melanie Volkamer, and Reto Koenig. Transparency and technical measures to establish trust in norwegian internet voting. In *International Conference on E-Voting and Identity*, pages 19–35. Springer, 2011.

[68] Kristjan Vassil, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel, and R. Michael Alvarez. The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. *Government Information Quarterly*, 33(3):453–459, 2016.

[69] Verified Voting. International internet voting. https://verifiedvoting.org/international-internet-voting/, 2021. [accessed 11-Oct-2021].

[70] Kushtrim Veseli. *Voting as a habit? Quantitative analyses of voting costs and turnout in direct democracy*. PhD thesis, University of Zurich, 2016.

[71] Melanie Volkamer, Oliver Spycher, and Eric Dubuis. Measures to establish trust in internet voting. In *Proc. of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV)*, page 1–10, New York, NY, USA, 2011. ACM.

[72] Jan Vom Brocke, Alexander Simons, Bjoern Niehaves, Kai Riemer, Ralf Plattfaut, Anne Cleven, et al. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *Proc. of the European Conference on Information Systems (ECIS)*, volume 9, pages 2206–2217, 2009.

[73] Merrill Warkentin, Shwadhin Sharma, David Gefen, Gregory M Rose, and Paul Pavlou. Social identity and trust in internet-based voting adoption. *Government Information Quarterly*, 35(2):195–209, 2018.

[74] Jane Webster and Richard T. Watson. Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly*, 26(2):xiii–xxiii, 2002.

[75] Jan Willemson. Bits or paper: Which should get to carry your vote? *Journal of Information Security and Applications*, 38:124–131, 2018.

[76] Alexandros Xenakis and Ann Macintosh. Trust analysis of the uk e-voting pilots. *Social Science Computer Review*, 23(3):312–325, 2005.

[77] Yu-Qian Zhu, Anik Hanifatul Azizah, and Bo Hsiao. Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries. *Information Development*, 2020.

[78] Verena Zimmermann and Nina Gerber. "If it wasn't secure, they would not use it in the movies"–security perceptions and user acceptance of authentication technologies. In *Proc. of the International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 265–283, Cham, Switzerland, 2017. Springer.

[79] Marie-Laure Zollinger, Verena Distler, Peter B. Roenne, Peter Y. A. Ryan, Carine Lallemand, and Vincent Koenig. User experience design for e-voting: How mental models align with security mechanisms. In *Proc. of the International Joint Conference on Electronic Voting (E-Vote-ID)*, pages 187–202. TalTech, 2019.

[80] Marie-Laure Zollinger, Ehsan Estaji, Peter YA Ryan, and Karola Marky. "Just for the sake of transparency": Exploring voter mental models of verifiability. In *Proc. of the International Joint Conference on Electronic Voting (E-Vote-ID)*, pages 155–170, Cham, Switzerland, 2021. Springer.

A Study Material

A.1 Study Invitation Text

The research group [Name blinded for anonymity] of the [University name blinded for anonymity] conducting an interview on the topic of "Internet voting".

What is it about?: The interview is about our opinion on Internet voting. No previous knowledge is required. However, participation is limited to subjects who have not participated in an election via the Internet.

Compensation: The participation will not be compensated.

A.2 Interview Guide

Welcome to our study on electronic voting conducted by the [name of research group blinded for anonymity]. In the course of this interview, I will ask you several questions. Participation in this study is voluntary. You may discontinue participation in the study at any time without giving a reason and without fearing negative consequences. The interview will take about 40–60 minutes.

In the interview, I will ask about your personal opinion, therefore there are no wrong answers. The data collected will be analyzed anonymously and parts of it may be published in scientific venues. Additionally, the interview will be audio-recorded electronically by this device. [Show device] Before analysis, the recording will be transcribed and anonymized. I will let you know when the recording starts and when it will stop. Please read this consent form carefully. If you have any questions about it, you can ask me directly. Once you are done, please sign the consent form and send it to me.

The study is divided into sections consists of the following components: your experience with voting, simulation of an electronic election, the main interview and two questionnaires which you can fill out on the computer.

If you have no more questions, I would start the audio recording now. Afterwards, please say that you agree with the recording. [Start audio recording] Do you agree with the audio recording? [Waiting for answer] To begin, I'll ask you a few general questions about political elections.

1) Experiences:

- Have you already voted in a political election, such as a parliament election?
- How did you participate in the last election? Did you vote in-person or by postal voting?
- Do you use this voting method often, or do you switch between methods?

- Try to remember the last elections in which you participated. Did you vote mostly by postal voting or by in-person voting? Which of the two methods did you use more often?
- Why did you choose the voting method you selected more often?
- What information channels do you use to learn about political elections? The focus here is on the election itself and not on the political program of the parties.
- Have you ever heard of electronic voting or Internet voting?
- Do you have an opinion about such electronic elections? If so, what is it?

2) Familiarization: Internet elections function similarly to traditional elections. However, the Internet is used to transmit the votes to an electronic ballot box, and counting also takes place via computer. At home, a computer or smartphone is typically used as voting device. In the following, I will simulate an Internet election for you so that you can get an idea of how an Internet election might be like. If you have questions about any of the steps, feel free to ask me. (Presentation is shown to participant. Screenshots are from Marky et al. [41].)

After you register with your Citizen's Office, you receive the following letter via postal mail a few days before the election. Please, read the letter carefully. If you have any questions about it, you can ask me directly. With a computer, you can cast your vote from any location. For identification, you use credentials from the letter. Then, you select the candidates or parties you want to vote for. After that, you can review your choice. If you do not want to change your choice, you click on seal and submit. Afterwards, you can verify your transmitted vote. For this you need a list of verification codes which is in our letter. This list has been generated individually for you and therefore contains different codes for each voter. Verify if the displayed codes match the codes from your list. If everything is correct so far, you enter your ballot insertion code. Then, you click "cast ballot". Finally, you will be shown a completion code. If everything was transmitted and deposited correctly, this will be identical to the completion code on your ballot. The purpose of verifying your vote is to make sure that your vote has been stored unchanged in the electronic ballot box. If there are any errors in your vote, you can contact the election office, e.g., by phone. Did you understand the Internet voting process? Please feel free to ask any questions you may have.

3) Trust Practices: There are several options for authorities to provide information to voters about the online voting system. Now we would like to know how the provision of the following mechanisms impact your personal trust in an Internet election. For this, I will show you possible mechanisms. After I introduced the mechanism, you can tell me if and how this impacts your personal trust.

- An examination of the voting software is carried out by independent experts in the fields of information technology and cybersecurity.
- Eligible voters are identified electronically, e.g., with the electronic identity card and a card reading device.
- You can verify the correctness of your own vote with the demonstrated electronic voting procedure.
- You have the possibility to change your own vote several times until the end of the election (this was not part of the simulation).
- The entire program code of the voting software (website and voting server) is publicly disclosed. This is also known under the principle "open source".
- You have the possibility to use a trial system to mark trial ballots before or at the same time as the actual election to familiarize yourself with the new system.
- Different interest groups, such as public organizations, trade unions or the political parties, may publish a voting software that you can choose for vote casting. In addition, there is an official election software from the Federal Election Commissioner.
- Information campaigns in public and private media (TV, radio, print advertising, social media) about electronic voting will be conducted.
- You can call assistance or access it online to clarify questions about electronic voting.
- Are there any other aspects that I have not mentioned that might increase trust in electronic voting?

4) End: Now, I would like to collect some demographic data from you. Please fill out the following questionnaire on the computer. Do you have any other questions or comments? With that, I thank you for participating in this study. I will end the audio recording now. If you have any questions at this time, please feel free to ask me.

B Codebook

Code	Description
mandatory	The practice is considered as essential during an online election
positive	The practice impacts the participant's trust in a positive way
neutral	The practice impacts the participant's trust in a positive way
negative	The practice impacts the participant's trust in a negative way
no clear option	The participant's statement is not related to their subjective trust or the question was skipped
misconception	The participant's trust assessment is based on a misconception
new	The participant stated an aspect that is outside the list of practices

Table 2: Codebook used to analyze the interviews.