Vote Secrecy and Voter Feedback in Remote Voting – Can We Have Both?

Arne Koitmäe[1], Jan Willemson[2][0000−0002−6290−2099], and Priit Vinkel[2][0000−0003−0049−1287]

[1] State Electoral Office, Lossi plats 1a, Tallinn, Estonia
[2] Cybernetica, Narva mnt 20, Tartu, Estonia

Abstract. The principle of secrecy is one of the most important tools to guarantee a voting process without undue influence to the voter. However, the concepts of the secret ballot and secret vote have strong ties to voting in a controlled environment in the polling station, and remote voting methods like postal voting or Internet voting need to employ special measures and approaches to achieve similar results. At the same time, limited options of observing the tallying process remotely potentially undermines the trust in remote voting. This paper looks at possible ways of giving the voter some feedback and assurance in the integrity of their vote, at the same time adhering to the freedom of voting principle. The Estonian Internet voting system is used as a model case for evaluation of a possible feedback channel architecture.

Keywords: Voting feedback, freedom of voting, secrecy of vote, Internet voting, remote voting

1 Introduction

Freedom of voting – the principle where the voter is able to cast his or her vote without undue influence – is one of the cornerstones of the democratic process. Secrecy of the vote is one of the most important tools to achieve this goal. However, the way we understand vote secrecy is closely related to the concept of traditional voting – the ballot is filled in privately in the voting booth, and then deposited into the ballot box. However, many voting methods also deviate from this scheme. One example is postal voting, where there is no control whether the ballot is filled in privately, and no solid guarantees can be given that the ballot sent through mail is not lost, opened, or tampered with.

In general, once the paper vote is cast in the ballot box (or the envelope with a ballot posted in mail) the voter has no way of verifying how their vote is processed and counted. Observation of voting and vote counting procedures are meant to ensure the integrity of the tally. While the voter's participation is recorded in the voter list and the data of the voter lists can be compared to the final tally, the path of the vote itself – anonymous ballot – is untraceable by the voter. This is usually not a problem if the trust towards the election management is high enough. However, it can be a problem if the trust is low,

especially if there are doubts about the elections being conducted in a free and fair way.

Internet voting (i-voting) provides new challenges when implementing ballot secrecy. A well-implemented i-voting system can use cryptography to guarantee that the ballot is sent and received as intended, with its integrity untouched. An observer or an auditor can make sure that all the votes cast are accounted for, that the votes included in the tally are the same as cast, and that the votes were tabulated correctly. However, voters themselves cannot fully verify i-voting results and people need to have absolute faith in the accuracy, honesty and security of the whole electoral system [38]. The path of their vote is something voters cannot trace or observe directly, and this can undermine the trust in the i-voting system. Trustworthiness of i-voting is more and more connected to additional confirmations given to the voter about the vote being handled correctly and processed as required by law.

However, the more information we give to the voter about their vote, the more the secrecy of the vote is undermined. In order to ensure freedom of the vote, it should not be possible to use this information against the voter. Secrecy of the vote should remain intact and voters should not find themselves in a weaker position against possible malefactors because their voting information is revealed.

Another problem in regards to i-voting and vote secrecy is the voting environment, which should ensure voter privacy. This cannot be guaranteed by election administration when the voter is voting from the location of their choice using a personal computer. Hence there are inherent risks present, like a possibility of malware tampering with the vote, or taking over the electronic identity used to authenticate the voter and sign the encrypted ballot. The worst-case scenario is that a malicious actor casts the vote using voter's electronic identity without the voter even knowing it. The observers and auditors cannot review how the vote was cast at the location of the voter. This presents a need for additional checks available to the voter. Merely the confirmation that the i-voting tally is verifiably correct doesn't address this concern. This concern is not limited to i-voting either.

Therefore it would be beneficial to give voters further confirmation about how their vote is handled with a goal to increase the trust in voting in general. Another issue to consider is that such measures should not make voting arrangements too complex for the voter, as not to restrict access to voting. In this paper we will examine whether this can be achieved without significantly weakening vote secrecy.

In order to have a more concrete treatment of the topic, we will be using Estonian Internet voting as the example case study throughout this paper. In the Parliamentary and European Parliament elections of 2019, the share of i-votes cast was 43.8% and 46,7% of participating voters, respectively [14]. Thus legitimacy of elections in Estonia very much hinges on the perceived trust of i-voting. Estonian i-voting system features both individual verification (introduced in 2013 [32]) and server-side auditing (introduced in 2017 [29]). Swiss and

Norwegian i-voting solutions have implemented individual and universal verification solutions as well. The Swiss Post e-voting solution uses verification of votes cast both individually by voters and universally by the electoral commission [17]. The Norwegian i-voting system used return codes for individual verification and server side auditing [26]. Individual verification is limited to confirming that the voter's vote was received as intended by the vote collecting service. Server-side auditing, on the other hand, allows to certify that the votes as a complete set have been tallied correctly. However, the popularity of i-voting in Estonia has initiated debate over 1) how freedom of vote and vote secrecy are guaranteed for Internet voting, and 2) what measures would increase general trust in the system [13]. Contributing to this discussion is the main motivation behind the current paper.

The paper is organised as follows. Section 2 presents a discussion on the concept of secret ballot that has been traditionally used to guarantee voting freedom. We also take a broader look at remote voting environments to understand how far is it reasonable to go with the vote secrecy requirement in this setting. Section 3 studies a possible additional feedback channel notifying the voter on the fact that a vote has been cast on their behalf. We analyse possible implementations of such a channel together with their impact on voting freedom. Finally, Section 4 presents some conclusions and sets directions for future work.

2 Concept of the secret ballot

2.1 Secrecy of the vote

Vote secrecy hasn't always been a requirement when conducting elections. Before mid-19th century it was rather a standard to vote openly, e.g. via stating one's preference out loud, or using visually distinguishable ballot sheets. Of course this also encouraged various coercive practices. To counter these, voting by secret ballot was introduced, with Australia being one of the first countries where it was systematically implemented [22, 41].

Today the requirement of vote secrecy has been stated in the highest level of international legislative acts. The United Nations International Covenant on Civil and Political Rights (UN CCPR) [3, Art 25], United Nations Universal Declaration of Human Rights [1, Art 21] as well as the European Convention of Human Rights (ECHR) [2, Art 3 of Prot I] state that voting shall be held by secret ballot. UN CCPR's General Comment 25 [4] adds that states should take measures to guarantee the requirement of the secrecy of the vote during elections, implying that voters should be protected from any form of coercion or compulsion to disclose how they intend to vote or how they voted, and from any unlawful or arbitrary interference with the voting process.

On electronic voting, Article 3.2 (iv) of the Council of Europe (CoE) Venice Commission's Code of Good Practice In Electoral Matters states that that the (electronic) voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage [6]. The CoE recommendation CM/Rec(2017)5 [12] on standards for e-voting makes several suggestions

towards maintaining vote secrecy. Article 23 of the Appendix to CM/Rec(2017)5 states that an e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties. Article 24 states that e-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.

The Code of Good Practice in Electoral Matters elaborates on the concept of secret suffrage on the voter's side as well. It states that for the voter, secrecy of voting is not only a right, but a duty as well. It also requires that voting must be individual, and that the list of persons actually voting should not be published [6, Art 4]. In the explanatory report, the Venice Commission explains that the purpose of the secrecy of the ballot is to shield voters from pressures they might face if others learned how they had voted [6, Par 52]. Moreover, since abstention may indicate a political choice, list of persons voting should not be published [6, Par 54].

From the voter's point of view, perceived vote secrecy is not necessarily equal to formal vote secrecy interpreted and implemented by the Electoral Management Body (EMB). The voters must also believe that the election administration operates in a way that their choices are kept secret (psychologically secret ballot) [27]. I-voting adds another dimension here, since the voters must additionally believe that other voters respect privacy and secrecy of the vote. Additionally, voters might feel socially obligated to reveal their votes, or they can believe that other voters might do so (social secrecy of the ballot) [27].

In the jurisprudence of the model case of Estonia, the current thinking regarding secrecy and Internet voting is based on the teleological approach, meaning that constitutional principles should be understood through the problems these principles were meant to solve [24]. It was first noted in 2004 as the underlying motivation for the draft legislation allowing for Internet voting [24]. In addition to that, the second source of the current approach is the liberal idea of trusting the voter [24, 36]. The principle of secrecy would protect an individual from any pressure or influence against her or his free expression of a political preference. Thus, the principle of secrecy is a means, not an end goal [24, 37]. Influence resistance in the Estonian i-voting system is guaranteed by the possibility of re-voting, thus the principle of secrecy, the end goal, is actually achieved [36]. This approach has now been generally accepted and expanded on [35, 37, 38] as not just the reasoning behind the original draft legislation, but as the actual explanation to how Internet voting conforms to the principle of secret ballot.

There remains a question whether the second part of reasoning – that the voter should be trusted – is applicable to the principle of secrecy. Vote secrecy cannot be understood as just optional, i.e. it's not just up to the voter to decide [19], but remote internet voting requires rethinking of the privacy principle [36, 37]. In support of a more traditional approach, Buchstein in 2004 (before the first i-enabled Estonian elections in 2005) argued for the sanctity of the secret ballot, while admitting that Drechsler's and Madise's interpretation and Estonian constitutional debate comes in as a possible starting point for a paradigmatic change [23]. There were also concerns that the transition towards voting

more from home, the concept of election may change without a real discussion on how that may weaken the voters' consciousness of a secret and personal vote [40]. This paradigmatic change has occurred, to an extent, when considering i-voting initiatives in Estonia, Switzerland and Norway, but also the raise in popularity of postal voting in general. The aforementioned countries have developed their i-voting system in line with the international standards and recommendations, while monitoring the experiences of other countries [21]. The updated CoE recommendation on i-voting CM/Rec(2017), now at its second iteration, reflects this change as well.

In practice vote secrecy on voter's side has been difficult to enforce, as many voters do not care about secrecy or do want to make their choice known, because of the social secrecy of the ballot as described by Gerber *et al.* [27].

2.2 Secrecy of participation in voting

Additional consideration should be given to how the principle of secrecy relates to voter's participation in voting. The Venice Commission has explained that voter lists with information on who voted shouldn't be published and abstention is a from of political choice [6, Par 54].

At the same time, when we look at voting as a general process, full participation secrecy is impossible to implement as voting in the polling station is public by nature. In regards to social secrecy of the vote, voters are often encouraged to participate and make their participation known by election stakeholders. This can possibly lead to problems in maintaining vote secrecy as well. For example, in Sweden, where ballots are printed separately for each party, party activists hand out ballots in front of the polling place to their voters. If the voter takes just one ballot, the content of the ballot is then known to bystanders [25].

The act of voting and content of the ballot are not approached the same way by voters and election stakeholders. As a result, voter lists (at least individual data of a voter) do not really fall under the umbrella of maintaining vote secrecy. In the past, personalised data on Internet voters has even been studied by researchers [35].

As for our model case of the Estonian Internet voting system, the current regulations stipulate that all data on Internet voters shared for scientific purposes must be made anonymous (including voting logs) [8, Par 77-1 (2)]. As for polling station voter lists that have been traditionally on paper, access to them is limited to the voters (personal information only) and parties; candidates and their representatives must justify why they need access (e.g in case of an elections dispute) [8, Par 23 (2)]. Additionally, the data can be used for scientific purposes. Thus the data concerning the voter is always available to the person without limitations, but the voter list data cannot be published or released to third parties except in cases stipulated by the law.

2.3 Challenges of keeping vote secrecy while increasing voter trust in the modern voting environment

A modern voting environment can include several methods of voting that differ in how much direct control the EMB has over it. Voting in a polling station takes place in a standardized environment, under control of the polling station staff. At the same time, the ballot box voting arrangements at home, overseas or at hospitals can be less convenient for the voter. On the other side of the spectrum are off-site voting methods like postal voting and Internet voting, being conducted without any supervision of the election administration. The vote delivery channel (mail or Internet) is in such cases not controlled by the EMB either.

If we accept that:

1. maintaining vote secrecy is not just the task of the EMB, but also of the voter,
2. not all ballots are cast under the direct supervision of election administration,
3. vote secrecy is just means to achieve the principle goal of free elections,

voters should also have the appropriate tools to be able to achieve that goal.

There are already a few measures at the disposal of the voter (with the implementation details varying across jurisdictions), e.g.:

- The voter can vote on the election day at a polling station and then observe the election procedures up to the end of vote counting. This gives a certain level of confidence that the voter's personal ballot (among other ballots) was not tampered with. Here the voter has to trust their own observation.
- Voters can check their data in the voter list, which includes information on whether they have voted, and possibly also the voting method that was used (i.e. Internet voting, voting outside the territory of their municipality or constituency). However, if the voter must personally access the voter list (or request the information from the EMB) then this requires action on voter's part and the voters must also be aware of the possibility. Therefore it is unlikely to provide any statistically significant amount of verifiability to increase trust in elections in general.
- An Internet voter could verify that the vote cast was received and stored as intended. There are several ways to implement this. For example, in Estonia, a smart device application is used for verification [32], but it does not help in the case when the voter is unaware that someone has cast a vote on their behalf. Since this method requires action on the voter's side, it hasn't achieved wide usage. The share of i-votes verified by the voters has remained between 4-5 per cent of all i-votes since 2014 [14]. It can be used to detect certain mass attacks against i-voting (e.g. when malware is trying to manipulate active voting sessions), but not all of them (e.g. when malware itself initiates the sessions without voter participation).

– In case of postal voting in Finland, the postal voter and the voting procedure have to be accompanied by two independent witnesses who could attest in writing that the freedom of vote and vote secrecy have been adhered to in this process [33, 39].

None of these measures undermine vote secrecy, but the problem is that these methods are limited in scope and they presume significant extra actions from the voters.

In order to certify one's vote, there are also other methods that are either discouraged by EMBs or not supported by legislation.

– Voters can take a photo of their ballots in the polling booth, or screen capture their choices in the Internet voting app or verification app. The voter can also live broadcast their voting from the polling booth [20]. This provides some (although quite a weak form of) proof that the vote has been cast correctly. This also lets the voter publish the image of the ballot taking, thus conflicting the vote secrecy principle.
– Voters can also mark their paper ballots in a way that it would be recognizable during the vote counting. If the voter (or some other informed party) then observes the count, they can make notice whether and how their vote was counted [42]. This is also possible for Internet voting, for example modifying the choice on the ballot in a way that the i-vote will be counted as invalid. As an example, there have been actual cases of sending in invalid votes in case of Estonian i-voting [30, 31].

The two above channels are violating the vote secrecy requirement, presenting proof of the contents of the ballot, thus making the voter more vulnerable to undue coercion. However, neither of the methods is something the EMB can directly block. In such cases it should be up to the legislation and EMB to determine if the act of vote is impermissible or the vote invalid.

In Finland, for example, the votes that contain extra markings on them are declared invalid by law [5, Par 85 (6)]. However, in Estonia, such a regulation does not exist. In fact the law stipulates that if the ballot is not filled correctly (e.g. the number of the candidate is not written on the correct spot), but the choice of the voter is otherwise understood (e.g. the name of the candidate was written on the ballot), the ballot is considered valid [8, Par 57 (6) 8)]. This presents an opportunity for the voters to get creative, enabling tracking of their votes. As for taking pictures of ballots (and publishing them), restricting these activities is even more complicated.

In the case of *stemfies* (ballot selfies), it is also apparent that the legislation and our general understanding of the secrecy have not kept up with the technological advancements [20]. It is unclear, whether and how such voter-initiated deviation from secrecy should be blocked and enforced by law, especially for remote voting. The consensus in this hasn't been reached yet. For example Section 56 (6) 5a of German Federal Electoral Regulations states that the Electoral Board must turn away any voter whom they find taking photos or videos in the

voting booth [7]. At the same time, in the Netherlands taking ballot selfies is allowed, although not encouraged [11]. *Stemfies* can also spark debate about other human rights and freedoms. European Court of Human Rights has ruled [15] that forbidding to use a mobile app to publish voter's ballot was in conflict with the Art 10 (Freedom of Expression) of the European Convention on Human Rights [2].

In summary, to improve voter's control over how voting is handled, we should be looking for a solution that wouldn't interfere with vote secrecy, give voters a way to verify their vote was handled correctly, and that would be universal enough to achieve statistically significant amount of checks.

A possible way to achieve the latter goal is to require as little action from the voter as possible. As we saw above, one of the main attack vectors not detected by the current verification mechanisms is malware that casts votes without the voter knowing about it. A similar problem occurs if the voter's eID is taken over physically. To detect such attacks, the system can be augmented with a feedback channel that gets triggered every time a vote is cast on voter's behalf. Next we will be studying the options of establishing such a channel.

3 Establishing a feedback channel

3.1 Feedback on the fact of casting a vote

When introducing a feedback channel, our goal is to give i-voters additional assurance that they have (or have not!) voted. On the other hand, we do not want to publish the proof in a way that it would render re-voting as a measure to maintain voting freedom inefficient.

Currently, the Estonian system allows to get feedback on several levels.

- Confirmation that the vote collecting service has received the i-vote and received it as intended. In Estonia this is currently implemented by the smart device verification app.
- Confirmation that the i-vote was included in the set of i-votes that are going to be tallied. Since the list of i-voters is created by the Internet voting system, a voter can check if their i-vote is included in this list, but this action is very inconvenient to the voters (see Section 2.3).
- Confirmation that the i-vote was amongst the i-votes tallied. Currently no feedback for the voter exists here, but the integrity of the i-vote set is verified by the EMB and auditors.
- Confirmation that the vote was counted as intended. Currently no feedback for the voter exists here, but the result can be verified by the tallying proof by the EMB, auditors and by anyone who has created an auditing application.

What is missing from this list is a passive method for getting information about the vote being received by the system. If such a feedback on voting participation only reveals the fact that the voter has voted at some point, then the clash with the principle of vote secrecy is minimal. It would, however, imply that

the voter has not abstained from voting. In such a way, giving a notification that a person has i-voted would be similar to situation when someone would take a photo of a voter leaving a polling station.

Introducing a voting fact feedback channel would benefit the voter in two main ways:

1. the voter would get assurance that the vote has been received and stored; and
2. even if the voter did not vote, absence of the voting notification would confirm that no-one else has voted for them.

Both confirmations would be useful to both i-voters and paper ballot voters. The assurance for the voter that no-one has cast a vote on their behalf can hopefully increase trust in the elections, including Internet voting.

Recall, however, that the ability to withstand coercion attacks relies on the possibility to cast re-votes in the Estonian system. Thus, assurance about which vote was processed (tallied) would potentially weaken the position of the i-voter, since this would reveal whether the coerced vote was later changed or not.

In conclusion, the feedback notification should just acknowledge the fact of receiving a vote by the system, but not much else (including the exact time, or the information whether it was a re-vote or not; see Section 3.3 for further discussion). Such a confirmation would be the most in line with the current legislation, not requiring to rethink how vote secrecy should be understood and protected.

In Estonia, such a system would be relatively easy to implement, since from 2021, electronic voter lists will be deployed. Amongst other features, it would enable the possibility to give voters automatic feedback whether they have voted, since this information is entered in the electronic voter list in real time.

Electronic voter lists make it possible for all (i.e. both paper and electronic) voters to receive such notifications. This is a positive outcome, since equal treatment of paper ballot and Internet voters has been a source of disagreement in Estonia before [9].

3.2 Setting up the feedback channel and automation

The method of giving feedback should be considered as well. The feedback channel should be set up in a way that the information is easily accessible only to the voter. At the same time, it should be universal enough so that as many voters as possible are able to get this confirmation. An example would be an e-mail or SMS sent to the voter. The message can contain just the notification on the fact of voting, or an access link requiring further identification (eID in Estonia's case).

The biggest advantage of using automated feedback is that it would notify the voters if their credentials have been used to cast the vote. So if the voter's electronic ID has been compromised and a vote has been cast on the voter's behalf, the voter would be notified immediately and would be able to take action.

In Estonia, one logical solution would be to use State Portal eesti.ee to store and send receipts, as already suggested in the 2020 study on feasibility of mobile voting [16]. This is accessible to every voter using eID, and every ID-card user gets automatically an e-mail address at eesti.ee. Eesti.ee also includes a mail forwarding service which residents can set up to forward this information their main e-mail address. Other government services and the Population Registry share the data about residents' contacts with eesti.ee portal, making the voter contact database fairly accurate and up-to-date [10].[3] An example of a current voting related service that uses eesti.ee portal is the possibility to order electronic voter cards instead of voter cards sent on paper by post.

Eesti.ee contact information enables to send messages to most of the voters, and the voters would get this information using their eID (recall that ID-cards in Estonia are mandatory). Hence, such a feedback method would be both relatively easy to implement and the message ("I voted") easy to understand. Since coercion-resistance measures can be difficult to implement or, indeed, difficult for the voters to understand [34], this is suitable as the next step towards giving voters more assurance about how their votes are handled. Using eesti.ee service as a gateway would also mitigate the problem that an attacker can send out fake notifications *en masse* [28].

3.3 Information provided by the feedback

As noted above, the Estonian re-voting scheme relies, amongst other features, on the element of uncertainty, assuming the malefactor has no way of knowing which was the last vote cast by the voter or whether the voter re-voted. This holds equally for both small- and large-scale coercion attacks (e.g. vote buying). Thus, it is important to give as much information as necessary and as little as possible in the feedback.

The electronic list of voters includes information on the date and time of voting, voting method used (including i-voting) and of course the fact of voting itself. Additionally, the voting system logs more data on the voter, including the age, the operating system used, IP-address etc. [18]. However, since we view the feedback channel as similar to checking voter's information in the list of voters, we restrict our interest to the types of information provided through this list only.

The minimal information included in the voting receipt would be the fact of voting, i.e. confirming that the person has been recorded as having cast a vote.

The method of voting used is another bit of information that is available in the list of voters, the most important distinction here being whether the voter voted over Internet or with a paper ballot. If we would provide this information,

[3] The COVID-19 pandemic had a positive side effect in this regard, forcing the government agencies to update people's contact information in order to send out vaccination calls. As of May 2021, 1,260,203 people in the Estonian Population Registry had a valid e-mail address, and 238,162 did not. This means that about 84% of Estonian residents can be reached by email.

it could reveal when the person re-voted with a paper vote, thus weakening the coercion resistance property. On the other hand, this information would give the voter assurance that their (i-)vote has not been changed.

It is also possible to send another confirmation after the voting period has ended, confirming that the voter's i-vote was entered into the count. This differs from checking one's data in the list of voters, since that information can be retrieved only from the Internet voting system before the votes are anonymized. Such information is unavailable at all for paper ballots, which become anonymous once inside the ballot box. This wouldn't reveal more information to the malefactor besides the method of voting, but would give the voter assurance that the i-vote was actually tallied (and not misplaced), which in turn would hopefully increase the trustworthiness of Internet voting to some extent.

Since our goal is to just give confirmation on participating in voting, precise date and time of the vote should not be necessary, although the benefit of giving the voter assurance that their last vote was the one tallied is significant. However, the precise time of the cast of vote might be construed as proof of casting a specific vote which would be advantageous to the malefactor.

3.4 Timing of the feedback

If the feedback is given during the voting period, this would give the malefactor a slight advantage, enabling them to coerce the voter to cast the vote again. If we do not include the date and time of voting in the receipt, the advantage for the malefactor is insignificant, essentially amounting to knowing that the person has voted at some point. Revealing the method used to vote or, for example, the date of voting (without the exact time) gives some additional information, showing possibly that an i-voter has re-voted in the polling station.

If the voting receipt is given after the voting period, then this would give the malefactor even less advantage, since the voter cannot re-cast the vote any more.

However, the advantage of giving feedback during the voting period is that it enables the voter to either re-vote if necessary, or file a complaint with a chance that the complaint will be resolved during the voting period. Instant feedback would also notify the voter if a vote has been cast using their credentials, thus exposing malicious takeovers of voters' electronic ID. If the complaint is filed after the end of the voting period, the voter has essentially no recovery mechanisms available. Even if the National Election Committee and/or the Supreme Court accept that the electoral law has been violated, the voter cannot cast a new vote after the voting has ended. The existing individual vote verification mechanism can be easily extended so that it would also provide a partial integrity check [28].

4 Conclusions and future work

The debate on the secrecy of vote has often concentrated on the fact of secrecy of vote itself, as if the secrecy is the definitive measure to guarantee free and

fair elections. This is certainly commendable, but one should not forget that the concept of secret ballot does not exist in a vacuum. "Old" Western countries take some justified pride in how the understanding of vote secrecy is ingrained in their society. However, this concept works well only for on-site voting, but the modern voting environment encompasses different popular voting solutions for off-site voting as well. We agree with the interpretation suggested by Madise *et al.* that vote secrecy is not the ultimate goal, rather than a necessary means to achieve free and fair elections. Vote secrecy is just one part of the equation. We need to maintain trust in the voting system by addressing other possible issues as well. Voters are more and more moving away from the polling places and off-site voting methods like postal voting, voting at home and i-voting gain more and more traction. It is inevitable that some conflict is built in here, but even so we must try to seek for a good balance in regards to vote secrecy and transparency.

One of the weak points is the voters' and observers' inability to observe and track the path of their ballot. In a way, i-voting has opened a Pandora's Box which made voters question voting methods and trustworthiness of elections in general. Whether aforementioned inability is real or perceived doesn't even matter, since trust is ultimately based on what people think, not what they are told by the election authority. Recent debates in Estonia (but also surely in many other countries) have shown the need to consider voter's trust in the system as a whole and to address these concerns. Therefore we propose to augment the system with a feedback channel allowing the voter to detect misuses of the voting credentials.

We recommend giving automatic feedback to voters on their voting: the method they used to vote as well as the day (but not the time) they voted. This would enable the voters to get assurance that their vote was cast and received as intended, that their vote was not changed later and, in case of abstention, no one voted using the voter's credentials. Making this feedback automatic (e.g. in Estonia through state portal eesti.ee) guarantees that most of the electorate will receive this notification, creating a new layer of verifiability for the system. The ballot count will still remain anonymous and a voter cannot link their vote to a counted vote, a necessary concession to support secrecy and coercion-resistance of the vote.

Establishing such an automated personal feedback channel to voters is not necessarily in conflict with the principle of secret suffrage when restricted just to the fact of voting. It is similar to a voter accessing one's data in the voter list, although the final verdict depends on the amount of data revealed. Determining a good balance between secrecy and transparency is a subject for further discussion. It would also seem that a feedback channel requires some amendments to the legislation, since it concerns processing voting data. Working out the exact nature of such amendments remains the subject for future research as well. We also hope that the debate over secrecy of the vote, what this entails and on how to handle this in a modern voting environment, will continue.

Acknowledgements This paper has been supported by the Estonian Research Council under the grant number PRG920. The authors are grateful to the Estonian Information System Authority and State Electoral Office for their support to the research process.

References

1. Universal Declaration of Human Rights (1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights, united Nations
2. European Convention on Human Rights (1950), https://www.echr.coe.int/documents/convention_eng.pdf, European Court of Human Rights
3. International Covenant on Civil and Political Rights (1966), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, united Nations
4. CCPR General Comment No. 25: Article 25 (Participation in Public Affairs and the Right to Vote), The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (1996), https://ccprcentre.org/page/view/general_comments/28883, united Nations Committee on Human Rights
5. Vaalilaki, last amended 1.01.2021 (1998), https://finlex.fi/fi/laki/ajantasa/1998/19980714, parliament of Finland
6. Code of Good Practice In Electoral Matters: Guidelines and Explanatory Report (2002), https://rm.coe.int/090000168092af01, European Commission for Democracy Through Law (Venice Commission)
7. Federal electoral regulations (2002), https://www.bundeswahlleiter.de/en/dam/jcr/e146a529-fd3b-4131-9588-8242c283537a/bundeswahlordnung_engl.pdf, bundestag
8. Riigikogu Election Act, RT I 2002, 57, 355; RT I, 03.01.2020, 2 (2002), https://www.riigiteataja.ee/en/eli/514122020002/consolide, parliament of Estonia
9. Constitutional judgment 3-4-1-13-05: Petition of the President of the Republic to declare the Local Government Council Election Act Amendment Act, passed by the Riigikogu on 28 June 2005, unconstitutional (2005), https://www.riigikohus.ee/en/constitutional-judgment-3-4-1-13-05, supreme Court of Estonia
10. Vabariigi Valitsuse määrus Eesti teabevärava eesti.ee haldamise, teabe kättesaadavaks tegemise, arendamise ning kasutamise nõuded ja kord, RT I, 25.03.2021, 5 (2013), https://www.riigiteataja.ee/akt/125032021005, government of Estonia
11. ECLI:NL:RBDHA:2014:5657, Rechtbank Den Haag (RBDHA) (2014), https://e-justice.europa.eu/ecli/ECLI:NL:RBDHA:2014:5657, court of the Hague, Netherlands
12. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017), https://https://rm.coe.int/090000168092af01, council of Europe Committee of Ministers
13. E-valimiste turvalisuse töörühma koondaruanne (2019), Estonian Ministry of Economic Affairs and Communications, https://www.mkm.ee/sites/default/files/content-editors/e-valimiste_tooruhma_koondaruanne_12.12.2019_0.pdf, in Estonian
14. Statistics about Internet voting in Estonia (2019), https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia
15. Case ECH-2020-1-002 Magyar Kétfarkú Kutya Párt v. Hungary (2020), http://www.codices.coe.int/NXT/gateway.dll/CODICES/precis/eng/EUR/ECH/ECH-2020-1-002, european Court of Human Rights

16. Mobile voting feasibility study and risk analysis (2020), report number T-184-5, Cybernetica AS, https://www.valimised.ee/sites/default/files/uploads/eng/2020_m-voting-report.pdf
17. E-voting: Online voting and elections (2021), https://www.post.ch/en/business-solutions/e-voting
18. Vabariigi Valimiskomisjoni otsus "Tehnilised nõuded elektroonilise hääletamise üldpõhimõtete tagamiseks", RT III, 27.01.2021, 6 (2021), https://www.riigiteataja.ee/akt/327012021006, estonian National Electoral Committee
19. Annus, T.: Riigiõigus. Juura (2006), in Estonian
20. Benaloh, J.: Rethinking voter coercion: The realities imposed by technology. In: 2013 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '13, Washington, D.C., USA, August 12-13, 2013. USENIX Association (2013), https://www.usenix.org/conference/evtwote13/workshop-program/presentation/benaloh
21. Binder, Nadja Braun Binder; Krimmer Robert; Wenda, G.D.H.F.: International Standards and ICT Projects in Public Administration: Introducing Electronic Voting in Norway, Estonia and Switzerland Compared. Halduskultuur: The Estonian Journal of Administrative Culture and Digital Governance **19(2)**, 8–21 (2019)
22. Brent, P.: The Australian ballot: Not the secret ballot. Australian Journal of Political Science **41**(1), 39–50 (2006)
23. Buchstein, H.: Online Democracy, Is it Viable? Is it Desirable? Internet Voting and Normative Democratic Theory. In: Kersting, N., Baldersheim, H. (eds.) Electronic Voting and Democracy: A Comparative Analysis, p. 97–108. Palgrave Macmillan UK (2004)
24. Drechsler, W., Madise, Ü.: Electronic Voting in Estonia. In: Kersting, N., Baldersheim, H. (eds.) Electronic Voting and Democracy: A Comparative Analysis, p. 97–108. Palgrave Macmillan UK (2004)
25. Elklit, J.: Is voting in Sweden secret? An illustration of the challenges in reaching electoral integrity. In: IPSA World Congress, University of Brisbane (2018)
26. Barrat i Esteve, J., Goldsmith, B., Turner, J.: Compliance with International Standards (2021), https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic4_assessment.pdf
27. Gerber, A.S., Huber, G.A., Doherty, D., Dowling, C.M.: Is there a secret ballot? Ballot secrecy perceptions and their implications for voting behaviour. British Journal of Political Science pp. 77–102 (2013)
28. Heiberg, S., Krips, K., Willemson, J.: Planning the next steps for Estonian Internet voting. In: Proceedings of E-Vote-ID 2020. p. 82 (2020)
29. Heiberg, S., Martens, T., Vinkel, P., Willemson, J.: Improving the Verifiability of the Estonian Internet Voting Scheme. In: Electronic Voting - First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016, Proceedings. Lecture Notes in Computer Science, vol. 10141, pp. 92–107. Springer (2016). https://doi.org/10.1007/978-3-319-52240-1_6
30. Heiberg, S., Parsovs, A., Willemson, J.: Log Analysis of Estonian Internet Voting 2013–2015. Cryptology ePrint Archive, Report 2015/1211 (2015), https://eprint.iacr.org/2015/1211
31. Heiberg, S., Willemson, J.: Modeling threats of a voting method. In: Design, Development, and Use of Secure Electronic Voting Systems, pp. 128–148. IGI Global (2014)
32. Heiberg, S., Willemson, J.: Verifiable internet voting in Estonia. In: 6th International Conference on Electronic Voting: Verifying the Vote, EVOTE 2014,

Lochau / Bregenz, Austria, October 29-31, 2014. pp. 1–8. IEEE (2014). https://doi.org/10.1109/EVOTE.2014.7001135
33. Jääskeläinen, A.: The Finnish Election System: Overwiew (2020), Oikeusministeriö
34. Krips, K., Willemson, J.: On practical aspects of coercion-resistant remote voting systems. In: International Joint Conference on Electronic Voting. pp. 216–232. Springer (2019)
35. Madise, Ü., Martens, T.: E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. In: Krimmer, R. (ed.) Electronic Voting 2006 – 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC, pp. 15–26. Gesellschaft für Informatik e.V., Bonn (2006)
36. Madise, Ü., Priit, V.: Constitutionality of remote internet voting: The Estonian perspective. Juridica Int'l **18**, 4 (2011)
37. Madise, Ü., Vinkel, P.: Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections. In: Kerikmäe, T. (ed.) Regulating eTechnologies in the European Union: Normative Realities and Trends, pp. 53–72. Springer International Publishing (2014)
38. Madise, Ü., Vinkel, P.: A judicial approach to internet voting in Estonia. In: E-Voting Case Law, pp. 135–158. Routledge (2016)
39. Nemčok, M., Peltoniemi, J.: Distance and trust: An examination of the two opposing factors impacting adoption of postal voting among citizens living abroad. Political Behavior pp. 1–25 (2021)
40. Vollan, K.: Voting in uncontrolled environment and the secrecy of the vote. In: Electronic Voting 2006–2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting. CC. Gesellschaft für Informatik eV (2006)
41. Wasley, P.: Back When Everyone Knew How You Voted. Humanities **37**(4) (2016)
42. Willemson, J.: Bits or paper: Which should get to carry your vote? J. Inf. Secur. Appl. **38**, 124–131 (2018). https://doi.org/10.1016/j.jisa.2017.11.007