E-Voting and the Law

Issues, Solutions, and a Challenging Question

Richard Hill

Hill & Associates, Geneva, Switzerland
rhill@hill-a.ch

Abstract. Governments have expressed much interest in e-voting, for various reasons including increasing participation, reducing costs, and facilitating absentee voting. E-voting systems based on the Internet have been implemented in various jurisdictions. Such systems have been criticized by technical experts. This paper first sets forth the threats to e-voting systems and the applicable legal norms. It then explains how technical solutions have been proposed or implemented to satisfy legal requirements. The paper notes that some criticism of e-voting systems is in reality criticism of remote voting in general; it notes that no remote voting system can be as secure and in-person voting, and that, if correspondence voting is accepted, then Internet voting can also be accepted provided that suitably secure systems are used. However, secure Internet systems are complex and rely on mathematical techniques that few can understand; this can result in lack of trust in such systems and voters might be reluctant to use them. The paper ends with a challenging question: should secrecy requirements be relaxed in order to allow deployment of simpler systems?

Keywords. E-voting. Internet voting. Legal issues.

1 Introduction

Voting, in the sense of people expressing a preference for one particular person or party, or proposal amongst a set of persons, parties or proposals, has a very long history, documented in writing since ancient times [1, 2]. Governments have expressed much interest in electronic voting systems, for various reasons including increasing participation, reducing costs, and facilitating absentee voting [3].

The use of machines to allow voters to cast votes and/or to count votes dates back to the middle of the 19th century, when devices that had the requisite capabilities were invented [1, 4]. Electronic voting machines have largely replaced mechanical voting machines [1]. Correspondence voting, that is, the casting of votes through the postal system without physically going to a polling station, also dates back to the 19th century: it was used in Australia in 1877 [5], and has gradually been extended, either only to allow non-resident voters to vote [6], or, as is the case in Switzerland [7], to allow all voters to vote from home.

A good overview of electronic voting is given in [8]. For the purposes of this paper, we will distinguish two types of electronic voting:

1. Use of machines in polling stations where voters vote in person.
2. Use of machines for casting (as opposed to merely counting) votes remotely (for example, Internet voting).

Both types above are used in practice and have been criticized for various reasons [3, 4], [9, 10, 11]. Type (1) above will be discussed only incidentally in this paper. The paper focuses on type (2), noting that much criticism of Internet voting is in reality criticism of remote voting, and then asks whether secrecy and/or anonymity might be relaxed in order to avoid technical complexities which most voters cannot understand. The question is relevant in light of proposed implementation of technical measures to improve the security of e-voting that are based on advanced mathematics. This paper does not attempt to provide an answer: its goal is to provide background information that could be useful when discussing the question in the future.

2 Threats and countermeasures

Any voting system is subject to threats, that is, to actions intended to manipulate voters, votes, counting or reporting of results [12]. Those threats can be grouped into two broad categories: manipulation of voters or votes; and manipulation of counting or reporting. Since counting and reporting are performed by electoral authorities, we can refer to these two broad categories as voter fraud and electoral authority fraud.

Voter fraud includes coercion, vote buying, replacing a voter's vote with a different vote, casting unauthorized votes (ballot stuffing), destroying a valid vote so it is not counted, etc.

Electoral authority fraud includes incorrect counting, whether deliberate or accidental, and incorrect reporting of correctly counted votes. In the case of electronic voting systems, such errors could be due to incorrect software programming and/or to malware introduced in the counting software.

Steps taken to counter threats, that is to minimize the likelihood of their influencing an actual vote, are called countermeasures. One of the most important, and commonly used, countermeasures is transparency: the voting process can be observed (either by anybody, or by selected observers), and so manipulations and fraud can be detected.

For example, the counting of votes can take place in a room open to the public, so that anybody who wishes to observe the process can see that votes are not being miscounted, or not counted. This countermeasure protects against electoral authority fraud.

Another example is the use of private booths in polling stations: voters mark ballots in private and cast their vote without anybody being able to see what the vote was. This countermeasure protects against coercion and vote buying.

One sees immediately that such countermeasures cannot easily be applied to electronic voting systems. For example, the traditional transparency countermeasure is difficult to apply for electronic voting: no form of automated counting can be fully observed and verified by ordinary voters. In Germany, constitutional requirements on the public nature of voting are such that it is very difficult to see how electronic voting could be implemented, whether for type (1) or (2) above [13].

Type (2) voting poses additional challenges: it is subject to all of the threats against correspondence voting (e.g. coercion, vote buying), but also to the threat of massive vote manipulation (e.g. by compromising the machines used by the voters).

Technical experts on electronic voting systems, electoral authorities, and the courts that enforce electoral laws have all addressed the question of what countermeasures are most appropriate in an electronic voting environment (see further discussion below). The threat of massive fraud is so significant that electronic voting systems experts have devoted much ingenuity and energy in developing countermeasures.

Those countermeasures include of course encrypting the transmission from the voter's machine to the electoral authority, but also much more sophisticated measures such as individual verifiability [14, 15, 16] and universal verifiability [17, 18] (these measures are explained below). Systems that implement individual verifiability are actually used in practice for national voting [19, 20, 21] and there are plans to deploy systems that implement universal verifiability [22].

It is important at this point to step back and summarize the legal requirements for any voting system, because of course electronic voting systems must conform to such requirements [23].

3 Legal requirements

National laws and regulations impose conditions on voting systems in order to ensure that they meet certain requirements, and that they implement countermeasures such as the ones mentioned above. We will summarize below scholarly writings on requirements (doctrine), laws and principles for electronic voting systems, and actual court cases related to electronic voting systems (case law). It is important to keep in mind that the crucial point is the binding legal norm. Doctrine can help understand and interpret legal norms, but not replace them. Depending on the legal system, the hierarchy of norms starts with binding/mandatory international law or national constitutional law, then laws enacted by parliament, then rules and regulations promulgated by the executive branch. Court decisions interpret the constitutional principles, laws, and regulations and apply them to specific cases. We start the discussion with doctrine, because it provides a good introduction to the legal requirements, and we include a reference to soft law (that is, to non-binding legal provisions) that support the doctrine. We then turn to laws and case law.

3.1 Doctrine and soft law

The legal and regulatory requirements for secure electronic voting are well summarized in [24]. In essence, the electronic voting system must ensure transparency, verifiability, accountability, and accuracy. It must guarantee the universal, free, equal, and secret character of elections. In more detail, the system must ensure (we list only those characteristics that will be further discussed in this paper):

1. That there is no coercion
2. One voter-one vote
3. Secrecy
4. Transparency
5. Verifiability and accountability
6. Simplicity

According to the cited work, secrecy is fundamental to the prevention of coercion (and vote buying), so "no voter should be able to prove that he/she voted in a particular way". As we will see below, this principle conflicts with the need to provide individual verifiability in Internet voting in order to counter the threat of malicious software in the user's computer. Further, as the cited work correctly notes, in correspondence voting "there can be no guarantee of the freedom from external influence by third parties during the casting of votes. This constitutes an inherent risk in any form of remote voting. To face this risk, measures should be taken on the policy and regulatory levels, in order to impose compelling and enforceable measures against coercion and to sanction illicit behavior. … Secrecy has to be in harmony with the other democratic principles for public elections. Ballot secrecy should be reconciled with transparency and auditability of the entire voting process."

Similar requirements are presented in [8], in addition of course to other characteristics that will not be discussed in this paper.

Another important source [25] of principles is the soft law (that is, non-binding legal provisions) developed by the Venice Commission. This document enunciates similar characteristics (in addition, again, to other characteristics). (This set of principles is reproduced in [26]). It is worth citing some of them verbatim:

1. Voting procedures must be simple.
2. Electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent.
3. For the voter, secrecy of voting is not only a right but also a duty, non-compliance with which must be punishable by disqualification of any ballot paper whose content is disclosed.

As shown below, condition (3) does not match either actual voter behavior, or actual laws, or certain court decisions. We will argue below that it is too strict and should perhaps not be imposed for Internet voting.

3.2 Laws and principles

The most comprehensive enunciation available at present at the international level regarding the legal requirements for electronic voting is without doubt the recommendation on the topic by the Council of Europe [27, 28, 29]. A discussion of the relation between the Council of Europe recommendations and national law is given in [30]. While the Council of Europe document is not international law, the principles that it enunciates are based on international law. Those principles are, for what concerns the present paper, essentially the same as those mentioned above.

National laws and regulations regarding electronic voting reflect the same principles [31]. However, some jurisdictions have developed detailed legal requirements, for example regarding individual and universal verifiability [32].

The issue of secrecy deserves special mention. Voting by raising one's hand in public is permitted in some jurisdictions, for example in some Swiss cantons: while the Swiss Federal Tribunal recognized that the secrecy of the vote was not guaranteed, it held that the traditional hand-raising public vote had other compensating characteristics so the freedom of the vote was not violated [33][1]. Other examples of non-secret voting exist, for example in Mexico [34]: "following traditional and ancient customs, Oaxaca's legal framework allows electoral procedures that do not protect the secrecy of the ballot."

We will return to the issue of secrecy in more detail later.

3.3 Case law

A comprehensive review of case law related to electronic voting systems is found in [31]. In essence, it can be said that courts are struggling with the issue of how to apply principles that are well understood for non-electronic voting systems to electronic voting systems. Court decisions range from essentially prohibiting electronic voting systems [13] to relying on the executive branch to ensure that electronic systems comply with the requirements mentioned above [32]. And from imposing [35] voter verified paper audit trails (VVPAT) to prohibiting [36] them (but the rationale for that particular decision is difficult to understand).

Difficult tradeoffs must be made between secrecy and verifiability, usability versus security, and costs. Such topics warrant considerable further inter-disciplinary discussions, because they relate to legal, technical, and social matters [37].

[1] The actual words of the Swiss Federal Tribunal, at the end of consid. 5(d) of BGE 121 I 138 are: "Die konkreten Unzulänglichkeiten des Abstimmungssystems an Landsgemeinden führen daher abstrakt gesehen nicht zu Wahl- und Abstimmungsergebnissen, welche den freien Willen der Stimmbürger nicht zuverlässig und unverfälscht zum Ausdruck brächten."

The remainder of this paper focuses on Internet voting systems, the specific tradeoffs involved in such systems, and their legal and social implications. Specific court cases will be cited below in specific contexts.

4 Internet voting

It is obvious that Internet voting, that is, the use of a voter's personal device connected to the Internet to cast a vote, is a form of remote voting. As such, it is subject to all the threats to remote voting, in particular coercion and vote buying. Correspondence voting systems (that is, sending paper ballots via the postal system) are of course subject to the same threats.

If a jurisdiction is not willing to accept the risks arising from such threats, then it is difficult to see how it can accept Internet voting, unless it has implemented multiple voting as a countermeasure against coercion and vote buying [19], [38, 39] (multiple voting is explained below).

On the other hand, if correspondence voting is accepted, then one has implicitly accepted the risks arising from coercion and vote buying. However, this does not mean that one has implicitly accepted the risks arising in Internet voting. Indeed, the most serious risk in Internet voting is not the coercion or vote buying directed against individual voters, but the risk of massive undetected manipulation of votes, for example by installing malicious software in the voter's personal device.

In the case of correspondence voting, individual voters must be coerced or bought, or, alternatively, individual paper ballots must be manipulated. In the case of Internet voting, it is possible to manipulate the computer systems to falsify the votes in such a way that neither the voter nor the electoral authorities can detect the fraud (see the previous citations to criticism of electronic voting systems). Unless of course individual verification is deployed and a significant number of voters check that their votes were received by the electoral authorities as cast. Indeed, individual verifiability is the primary counter-measure against massive fraud in Internet voting. (Individual verifiability is explained below.)

4.1 Legal requirements and technical solutions

The table below shows how specific technical solutions have been developed and implemented to satisfy (or not) the specific legal requirements mentioned above.

Requirement	**Technical solution**
Absence of coercion	Multiple voting
One voter-one vote	Voter identification
Secrecy	Encryption
Transparency	System audits, publication of source code
Verifiability and accountability	Individual and universal verifiability, system audits
Simplicity	

Individual verifiability (explained below) is used in Internet voting as a countermeasure to the threat of malicious software being present in a voter's personal computer or in the network connecting the voter's computer to the central server. But a consequence of individual verification is that a voter has evidence of his or her vote, and could be forced to reveal that, for example to a vote buyer. Multiple voting is a countermeasure to that threat. In multiple voting a voter can vote many times, and can use different channels. So a voter might vote one way using the Internet and show the receipt of the vote to a third party, but the voter could then change his or her vote unbeknownst to the third party by voting again, either via the Internet, or in person at a conventional polling station. Thus a person who seeks to coerce voters (or to buy their votes) cannot know whether the coercion (or vote buying) was successful.

Voter identification is achieved either by issuing machine-readable identification cards to voters, who use them to authenticate themselves when voting; or by sending a voter identification card containing a unique identifier to each voter for each vote via a separate channel that is held to be secure (e.g. the postal system): voters use the unique identifiers on the voter identification cards to authenticate themselves when voting; or by requiring that the user log into the voting system with a password (and possibly additional security measures such as challenge-response). As is the case for correspondence voting, there is no way to prevent a voter from giving his or her identification card, or unique identifier, or password, to another person, who would then vote in his or her place, unless biometric techniques are used in addition. (In some Swiss cantons, the voter must sign the voter identification card when voting by correspondence, so there can be a biometric check for postal voting – but in most cantons there is no systematic signature verification. There is no biometric check for Internet voting; however, even for the postal vote, there is no way to prevent the voter from giving the signed voter identification card to another person who will then vote in his or her place. Such activities are of course illegal and seem to occur rarely in Switzerland: there have been isolated instances of convictions for such activities.)

Encryption is used to ensure that the votes are not read (or changed) as they are transmitted from the voter to the electoral authority. Further, an electronic equivalent of the well-known double envelope technique is used to ensure that the actual vote is separated from the voter identification before the actual vote is decrypted and counted, so that the electoral authorities cannot know how voters actually voted.

In individual verifiability, the voter is given a pre-computed return code together with the ballot, through a secure communication channel such as the post. When the voter casts his or her vote, the central voting system sends back to the voter a return code. If the two codes match, then the voter knows that his or her vote was received correctly. This technique is a countermeasure to the presence of malicious code in the voter's computer and/or in the communication path between the voter and the central voting system.

In universal verifiability, all the votes are published, but after being scrambled in such a way that the votes are no longer associated with voter identities. Anybody can then verify that the votes have been counted correctly and that the published report of the vote is correct. This technique is a countermeasure to the presence of malicious software in the central voting system, and also a countermeasure against insider manipulation by the electoral authorities.

Transparency is achieved by publishing the source code, but this is not always done: some systems are proprietary and their source code is not published. On the other hand, all systems are subject to audits by electoral authorities and/or committees whose members are not electoral authorities and who are named by political parties or by other means. Such audits can include examination of the source code, review of the procedures used to install, test, and operate the voting system, test runs using test voting districts, etc.

Electronic voting systems are by nature complex, so simplicity cannot really be achieved, unless the requirement of simplicity is restricted to the user interface: the inner workings of electronic systems are necessarily complex and cannot easily be understood by the average voter (see [13]). This is in particular the case for universal verifiability, which relies on complex mathematical techniques. However, at the end of this paper, we pose a challenging question regarding whether less complex systems can be accepted.

4.2 Comparison to traditional voting

As noted above, the countermeasure of individual verifiability increases the risk of voter coercion or vote buying (unless multiple voting is allowed).

But are traditional polling stations immune to coercion or vote buying? The standard answer to that question is “of course, because the ballot is filled in privately and kept secret, so the voter cannot prove to a third party how he or she voted.” First of all, the prevalence of smartphones makes it easy for a voter to provide a record of how he or she voted (it does not appear practical to implement systems that would detect hidden smartphones or small cameras, and, at least in one jurisdiction, such practices are not forbidden [40]). More importantly, there is no reason to believe that voters who are willing to sell their vote would cheat and not vote as the buyer intended.

Further, traditional polling stations are not immune to massive fraud: there is no defense (other than criminal prosecution) against corrupt polling station officials, who can replace an urn with a pre-stuffed urn, in particular if the urns are transported for central counting. Of course public observation of the operations at the polling stating, the transportation of the urns, the opening of the urns, and counting of votes is a counter-measure to this threat. But, in practice, the threat remains real, and in fact the use of electronic machines in polling stations has been considered a better countermeasure than public observations in some jurisdictions where the risk of fraud by the electoral authorities is considered to be high [41].

Careful consideration of the criticism of Internet voting shows that much of it is in fact criticism of remote voting in general, that is, it applies also to correspondence voting. And it is based on the belief that voting in person, in polling stations, is inherently less risky that remote voting. For example [42] states (author’s translation): “But voters who cast their votes via the Internet using an ordinary computer connected to the global network do not benefit from the protection of a secret polling booth within a polling station. They are therefore susceptible to external pressure (from their family, from their hierarchical superiors, from their colleagues, etc.), just as is the case for any correspondence vote". Similar comments are made in [9], which heavily criticizes Internet voting systems, including systems with individual verifiability, and goes on to state: "Postal voting, as any system that allows a voter to cast a vote outside a voting booth, still has the disadvantages that voters can be coerced or paid to vote in a certain way. The possibility of repeated voting could reduce this problem. By going to the polling place after giving the Internet or postal vote, one has the opportunity to vote again. However, a patriarch of a closely controlled family could easily restrict his daughter's movements on the final day of the election, just as he could control their Internet voting. For those buying votes it is just a small calculated risk that the seller of the vote will turn up on Election Day." And [43] identifies as a major challenge to Internet voting "how to avoid voter coercion and vote selling in the context of digital observation of voting and verification". The same study includes expert statements such as "Remote voting entails significant risks above and beyond those of in-person poll-site voting. Included among these are risks to integrity – as remotely-cast ballots may pass through numerous hands without independent observation – and risks to privacy – as voting takes place without the benefit of publicly-enforced voter isolation."

Note that such criticism discounts the possibility that the result of a vote might be affected by threats against citizens who go to polling stations. In conflict areas, it is not uncommon to threaten anybody who votes, and anybody who votes in person can, in principle, be seen when he or she goes to the polling station. This threat to in-person voting is particularly significant when a quorum is required. In contrast, there is no obvious way to tell whether a voter has voted by correspondence, so remote voting may be more secure in such circumstances.[2]

The experts cited above go on to state that "Internet voting substantially exacerbates the risks of remote voting by making it possible for small problems to be magnified and replicated on a large scale. Careless or malicious errors, intrusive malware, and unforeseen omissions – all of which can be caused by individuals or very small groups – can cause very large numbers of votes to be changed and the privacy of large numbers of voters to be compromised." This is of course correct, and is the reason for the implementation of countermeasures such as individual and universal verifiability. But it is also the case that careless or malicious errors and unforeseen omissions – all of which can be caused by individuals or small groups such as election authorities – can cause large numbers of votes to be invalid or miscounted in traditional voting systems. So the criticism voiced by the experts is also applicable to traditional voting systems.

A severe criticism of the Estonian system [10] includes the following findings: "inadequate procedural controls", "lax operational security", "insufficient transparency", and it explains how the computers used by the electoral authorities to count the votes (the servers) can be compromised, for example by a dishonest insider or by using zero-day exploits (such as bugs in the operating system). But all those shortcomings

[2] I am indebted to Uwe Serdült for the observations in this paragraph.

could also affect a traditional voting system, so it is difficult to understand why it would be better "that Estonia discontinue use of the I-voting system" rather than that it focus on addressing weaknesses and improving the system to make it more secure, in particular by introducing universal verifiability.

In other words, why should we require that an Internet voting system be more secure than a correspondence voting system, if the jurisdiction allows correspondence voting? The Mexican electoral court has assumed that, as [34] puts the matter: "in certain circumstances, neither freedom [from external influences] nor ballot secrecy are sacred principles anymore, as they are often perceived within certain electoral contexts."

More controversially, why do we require that voters cannot voluntarily use systems in which the secrecy of the vote is not fully guaranteed?

5 A Challenging Question

The question "why not allow voters to use, if they wish, an alternative voting channel that does not fully guarantee secrecy" may sound like anathema at first reading, but no jurisdiction prohibits voters from voluntarily telling others how they voted. Of course in traditional in-person voting the voter cannot prove how he or she voted (unless the voter uses a smartphone in the private polling booth), but why would anybody doubt that a person is lying when he or she voluntarily reveals his or her vote?

The reality is that, at least in Western democracies, many people freely discuss with friends and family how they intend to vote, and do vote as intended. Further, influential people make public statements regarding their voting intentions, as part of election/voting campaigns (e.g. Mrs X will endorse candidate Y, or, in the case of referendums "I will vote against proposal Z").

And voters frequently participate in campaign meetings or rallies and/or in demonstrations. Such events are often publicly broadcast, so those voters have revealed their strong voting preferences, and thus it can be assumed that they will vote in accordance.

According to the case law of one jurisdiction (Mexico) secrecy is an individual right, not something to be imposed by the state in all circumstances. As [34] puts the matter: "In relation to ensuring freedom and secrecy, the Court finds an individual right in these guarantees, that is to say, governments would not be obliged to ensure that any ballot is cast secretly. They only have to provide a procedural framework where such an option becomes feasible." The same approach has been taken by the Estonian Supreme Court, which also considered that secrecy is a mere option available to the voter [34], citing [39].

As [33] puts the matter, referring to Swiss law, the main purpose of the secrecy of the vote is to protect the voter against attempts by the state to know how he or she voted. In contrast, the secrecy requirement is less strict for what concerns disclosure of the vote to a third party, if the voter has consented to such disclosure.

As noted above, and by the Mexican court, the threats of coercion and vote buying exist for all types of remote voting, not just Internet voting. But as [34] correctly points out, Internet voting is different from traditional correspondence voting, so the risks arising from threats can be significantly greater, and the countermeasures that should be taken might be different (for example, multiple voting is a countermeasure implemented for Internet voting).

As mentioned above, sophisticated techniques have been developed to counter the threats to Internet voting, specifically individual and universal verifiability. But these techniques rely on complex mathematical techniques (public key encryption, zero-knowledge proofs [44], MixNets [45], etc.) which most voters cannot understand, much less verify.

Thus such techniques cannot be used in countries that require, as does Germany [13], that any voter must be able to observe and understand the voting process, and verify that it has been correctly implemented.

As [24] puts the matter: “Voters should be able to understand how the elections are conducted.” This is the case for traditional voting systems, but not for electronic voting systems. As a consequence, voters unable to understand the complex techniques mentioned above may be reluctant to cast their votes using the Internet, thus defeating the reason for the implementation of an Internet voting system. As [8] puts the matter: “Lack of transparency with electronic voting and counting technologies means that confidence in the operation of the technology is a considerable problem.”

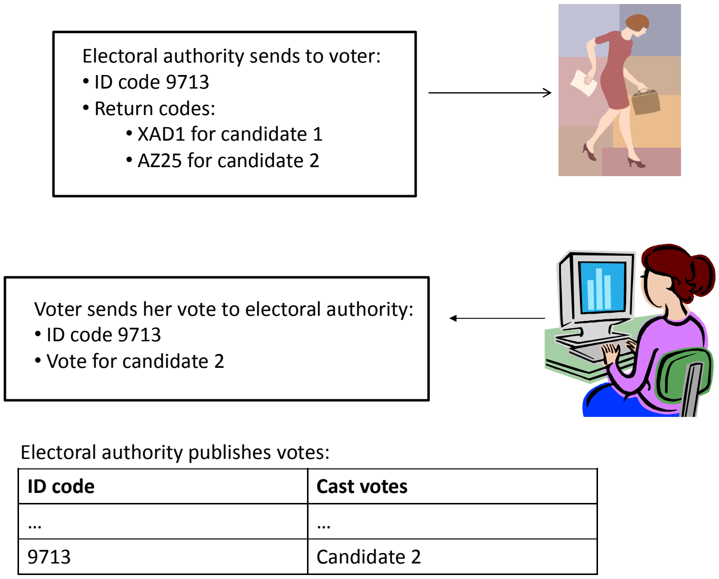
An alternative to these techniques would be to make available to voters a less technically complex Internet voting channel that does not fully guarantee secrecy, with the understanding that voters would be free to use other voting systems that do guarantee secrecy, for example in-person voting at a polling station or postal voting.

An example of such a system would be a system that implements individual verifiability, and in which the cast votes are published on the Internet. There would be no need to associate a cast vote with the name or personal identification number of the voter. It would suffice to associate the cast vote with a unique identification created for each election and transmitted to the voter together with the ballot. (We will use the term “election” to refer to a specific instance of voting, even if the voting in question is a referendum – a choice between alternatives – rather than an election properly speaking – a choice between candidates).

That is, the voter’s ballot would contain a unique identification generated for the particular election (it would change for each election), as well as the return codes that the voter should check after casting the Internet vote. The electoral authorities would publish on their web site the list of election-specific identification codes, and associated cast votes, for those voters that have chosen to vote via the Internet.

All of those voters could then check that their votes were recorded as intended, everybody can recount the cast votes, and everybody can check that that the reported results correspond to the cast votes, so universal verifiability is achieved. And nobody could see how those voters voted unless the voter reveals his or her unique election-specific identification code. The secrecy of the vote is protected unless the voter chooses (or is forced to) reveal that element.

The proposed system can be illustrated by the example below (the ID code is election-specific: it changes for each election):



Electoral authority sends to voter:
- ID code 9713
- Return codes:
  - XAD1 for candidate 1
  - AZ25 for candidate 2

Voter sends her vote to electoral authority:
- ID code 9713
- Vote for candidate 2

Electoral authority publishes votes:

ID code	Cast votes
…	…
9713	Candidate 2

Fig. 1. Proposed Internet voting system

The alert reader will recognize that, in such a system, there is actually no need for the return codes. The voter can directly verify that his or her vote was correctly received by the central system by consulting the published votes. But this implies that, if real-time verification by the voter is desired, then the votes would be published as they are received, which may not be desirable. Further, voters might be more willing to check a return code that is sent to them immediately after they vote, than to make the effort to go check the results published by the electoral authority. Thus it might be better to keep the return codes typically used in systems that implement individual verifiability.

The system outlined above does not protect against coercion or vote buying, so it is less secure than other types of Internet voting. And, if the voter chooses to use that system, it provides proof of how a voter voted. As noted above, providing proof by means of a selfie taken in a polling station is not prohibited in some jurisdictions [40], but the laws would likely need to be changed or clarified in other jurisdictions, in particular to make it clear that providing proof in exchange of payment would be illegal, as would be to coerce proof.

On the other hand, the system outlined above is far easier to implement and to verify, and voters may be more willing to trust such a system than a system that relies on complex mathematical techniques such as zero sum proofs and MixNets. And any massive campaign to coerce voters, or to buy votes, would likely be detected, as is the case at present for correspondence voting, because a large number of people would necessarily be involved, and it would be very difficult to keep the campaign secret. Indeed, the proposed system is no less secure than correspondence voting, because in correspondence voting the ballots can be bought, or the voter can be coerced to fill in the ballot in a certain way.

As already mentioned, a system that is not fully secret might be held to be constitutional in some jurisdictions, provided of course that voters have the choice to use another system that guarantees the secrecy of their vote, such as correspondence voting.

Would ordinary voters (that is, those who are not technical specialists) trust (and consequently use) such a system more than a complex system based on zero-knowledge proofs and MixNets? Empirical research seems to indicate that, not surprisingly, voters are more likely to trust a voting system that they can observe and understand [46, 47], and learned authors reach the same conclusion [48]. In practice, lack of trust can lead to abandoning electronic voting [49].

The question of whether voters would be more likely to trust, and use, a less mathematically complex Internet voting system is a sociological question, but it is an appropriate question. As [37] puts the matter: "… a multidisciplinary approach remains crucial. Social research linked to e-voting for example would be very useful to nuance and balance technical and legal conclusions".

Perhaps such social research could include the investigation of voter acceptance of the sort of non-secret Internet voting system outlined above, and revisit the tradeoffs between secret and open (that is, non-secret) voting methods [50, 51, 52].

In any case, the duties of electoral authorities with respect to secrecy would have to be specified, for example to provide information to voters regarding the risks of waiving their right to a secret vote; and to monitor possible attempts to buy votes or to coerce voters.

6 References

1. D. W.Jones: A Brief Illustrated History of Voting, The Voting and Elections Web Pages (2003) http://homepage.divms.uiowa.edu/~jones/voting/pictures/
2. J. J. O'Connor, and E. F. Robertson: The history of voting. School of Mathematics and Statistics, University of St. Andrews, Scotland (2002) http://goo.gl/4WVbgS
3. A. Driza Maurer: New Technologies: Inescapable but Challenging. 1st "Electoral Expert" debates on "Electoral Law and New Technologies: Legal Challenges", 12-13 April 2016, Bucharest, Romania. In Electoral Expert, forthcoming
4. D. W. Jones and B. Simons: Broken Ballots: Will Your Vote Count?, University of Chicago Press, Chicago, USA (2012)
5. M. Sawer, N. Abjorensenm and P. Larkin: Australia: The State of Democracy. Federation Press, pp. 107–114 (2009)
6. M. Germann and U. Serdült: Internet Voting for Expatriates: The Swiss Case,JeDEM, eJournal of eDemocracy & Open Government, vol. 6, no. 2, pp. 197-215 (2014) http://goo.gl/F24zc1
7. A. Driza Maurer: Internet Voting and Federalism: The Swiss Case. Revista General de Derecho Público Comparado, No. 13, 2013. And in J. Barrat (ed.): El voto electronico y

sus dimensiones juridicas: entre la ingenua complacencia y el rechazo precipitado, Iustel, Madrid, Spain (2015)

8. B. Goldsmith: Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies, International Foundation for Electoral Systems (2011) `http://goo.gl/7n8qlF`
9. K. Olsen and H. Nordhaug: Internet Elections: Unsafe in Any Home?. Communications of the ACM, vol. 55 no. 8, p. 36
10. D. Springall et al.: Security Analysis of the Estonian Internet Voting System, CCS'14, November 3–7, 2014, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (2014) `https://goo.gl/iJzYT1`
11. L. Loeber: E-Voting in the Netherlands: From General Acceptance to General Doubt in Two Years. In R. Krimmer, and R. Grimm, Ruediger (eds), Proceedings of the 3rd international Conference on Electronic Voting, GI-Edition, p. 21 (2008) `http://goo.gl/TVZpMz`
12. J. A. Halderman, J. Alex: Security Analysis of the Estonian Internet Voting System. Presentation at VoteID 2015, 2-4 September 2015, Bern, Switzerland (2015) `http://goo.gl/nsmLYr`
13. S. Seedorf: Germany: The public nature of elections and its consequences on e-voting. In [31]
14. R. Oppliger: Traitement du problème de la sécurité des plate-formes pour le vote par Internet à Genève, Chancellerie du canton de Genève, Geneva, Switzerland (2002) `http://goo.gl/t8o9gG`
15. J. Barrat, M. Chevallier, B. Goldsmith, D. Jandura, J. Turner, and R. Sharma: Internet Voting and Individual Verifiability: The Norwegian Return Codes. In M. J. Kripp, M. Volkamer, R. Grimm (eds): 5th International Conference on Electronic Voting 2012 (EVOTE2012), Proceedings, 11-14 July 2012, Bregegz, Austria (2012)
16. U. Madise and P. Vinkel: A Judicial Approach to Internet Voting in Estonia. In [31]
17. E. Dubuis, R. Haenni, and R. Koenig: Konzept und implicationen eines verifizierbaren Vote Eletronique Systems. Berner Fachhochschule, Bern, Switzerland (2012) `http://goo.gl/pj7Gyl`
18. E. Dubuis, S. Fischli, R. Haenni, U. Serdült, and O. Spycher: A Verifiable Internet Voting System. In CeDEM'11, Conference for E-Democracy and Open Government, pages 301-312, Krems, Austria (2011)
19. U. Madise, and T. Martens: E-voting in Estonia 2005: The first practice of country-wide binding Internet voting in the world. In R. Kimmer: Electronic Voting 2006, 2nd International Workshop, 2-4 August 2006, Bregenz, Austria, GI-Edition, p. 15 (2006) `http://goo.gl/dGB0xp`
20. Swiss Federal Chancellery: Vote électronique `http://www.bk.admin.ch/themen/pore/evoting/index.html?lang=fr`
21. D. Galindo, S. Guasch and J. Puiggali: 2015 Neuchatel's Cast-as-Intended Verification Mechanism. In R. Haenni, R. E. Koenig and D. Wikstrom (eds): E-Voting and Identity, 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4 2015, Proceedings, Springer (2015) `http://goo.gl/q7qss6`
22. Swiss Federal Council: Report on electronic voting, June 2013 `https://goo.gl/khhfhV`
23. A. Driza Maurer: Legality, Separation of Powers, Stability of Electoral Law: The Impact of New Voting Technologies. 1st "Electoral Expert" debates on "Electoral Law and New Technologies: Legal Challenges", 12-13 April 2016, Bucharest, Romania. In Electoral Expert, forthcoming

24. L. Mitrou, D. Gritzalis, S. Katsikas and G. Quirchmayr: Revisiting legal and regulatory requirements for secure e-voting. In D. Gritzalis: Secure Electronic Voting, Springer (2003)
25. European Commission for Democracy Through Law (Venice Commission): Code of Good Practice in Electoral Matters, Opinion no. 190/2002, CDL-AD (2002) 23, 2002 http://goo.gl/xrtLQj
26. European Commission for Democracy Through Law (Venice Commission): Electoral Law, CDL-EL(2013)006 (2003) http://goo.gl/HZuwbH
27. Council of Europe: Legal, Operational, and Technical Standard for E-Voting, Recommendation Rec(2004)11 (2004) http://goo.gl/9Eljv4
28. R. Stein and G. Wenda: Ten Years of Rec(2004)11: The Council of Europe and E-voting. In: R. Krimmer and M. Volkamer (eds) Proceedings of Electronic Voting 2014 (EVOTE2014), TUT Press, Tallinn, pp. 105-110 (2014) http://goo.gl/6IBpUi
29. A. Driza Maurer: Ten Years Council of Europe Rec(2004)11: Lessons Learned and Outlook. In: R. Krimmer and M. Volkamer (eds) Proceedings of Electronic Voting 2014 (EVOTE2014), TUT Press, Tallinn, pp. 111-117 (2014) http://goo.gl/RPCThl
30. A. Driza Maurer: Update of the Council of Europe Recommendation on Legal, Operational and Technical Standards for E-Voting – A Legal Perspective. Jusletter IT, 25 February 2016 (2016)
31. A. Driza Maurer and J. Barrat (eds.): E-Voting Case Law: A Comparative Analysis, Ashgate, Farnham, UK (2015)
32. B. Kuoni: Case Law on E-Voting – A Swiss Perspective. In [31]
33. A. Auer, G. Malinverni, and M. Hottelier: Droit constitutionnel suisse, Staempfli, Bern, Switzerland, Volume I, paragraphs 881-883 (2006)
34. J. Barrat: The Internet Voting Project in the Mexican Courts. In [31]
35. R. Bailey and R. Sharma: E-Voting Case Law in India. In [31]
36. A. B. Filho and A. Tavares Rosa Maracacini: Legal Aspects of E-Voting in Brazil. In [31]
37. A. Driza Mauer and J. Barrat: Conclusions. In [31]
38. S. Heiberg, P. Laud, J. Willemson: The Application of I-Voting for Estonian Parliamentary Elections of 2011. In: Kiayias, A., Lipmaa, H. (eds.) VOTE-ID. Lecture Notes in Computer Science, vol. 7187, pp. 208–223. Springer (2011)
39. U. Madise: Legal and Political Aspects of the Internet Voting: the Estonian Case. In J. M. Reniu Vilamala (ed), E-Voting: The Last Electoral Revolution, ICPS, Barcelona, pp. 45-60 (2008)
40. L. Loerber: E-voting in the Netherlands; past, current, future? In: R. Krimmer and M. Volkamer (eds) Proceedings of Electronic Voting 2014 (EVOTE2014), TUT Press, Tallinn, pp. 43-46 (2014) https://goo.gl/sX0neR
41. R. Martinez Dalmau : Venezuela : Finding the Relationship between E-Voting and Democracy. In [31]
42. C. Enguehard : Introduction à l'analyse de chimères technologiques, le cas du vote électronique. Cahiers Droit, Sciences & Technologies, Editions du CNRS, 3, pp.261-278 (2010)
43. J. R. Kiniry et al.: The Future of Voting: End-to-End Verifiable Internet Voting. US Vote Foundation, p. 108 (2015) https://goo.gl/fieXN1
44. P. Locher and R. Haenni: Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. In R. Haenni, R. E. Koenig and D. Wikstrom (eds): E-Voting and Identity, 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings, Springer (2015) http://goo.gl/0JsPIB
45. P. Bibiloni, A. Escala, and P. Morillo: Vote Validability in Mix-Net-Based eVoting. In R. Haenni, R. E. Koenig and D. Wikstrom (eds): E-Voting and Identity, 5th International Con-

ference, VoteID 2015, Bern, Switzerland, September 2-4 2015, Proceedings, Springer (2015) `http://goo.gl/VHYlWQ`

46. L. Caporusso: The Role of Trust, Participation and Identity in the Propensity to e- and i-vote. In: R. Kimmer and R. Grimm (eds): Electronic Voting 2010 (EVOTE2010), Proceedings, 21-24 July 2010, Bregenz, Austria (2010) `https://goo.gl/lbSJfE`
47. N. Boulus-Rodje: Mapping the Literature: Socio-cultural, Organizational and Technological Dimensions of E-voting Technologies. In M. J. Kripp, M. Volkamer, R. Grimm (eds): 5th International Conference on Electronic Voting 2012 (EVOTE2012), Proceedings, 11-14 July 2012, Bregenz, Austria (2012) `hhttp://goo.gl/PqJr1H`
48. O. Spycher, R. Haenni and E. Dubuis: Theoretical and Practical Implications of E-Voting. In: R. Kimmer and R. Grimm (eds): Electronic Voting 2010 (EVOTE2010), Proceedings, 21-24 July 2010, Bregenz, Austria (2010) `https://goo.gl/lbSJfE`
49. T. Hall and L. Loeber: Electronic Elections in a Politicized Polity. In: R. Kimmer and R. Grimm (eds): Electronic Voting 2010 (EVOTE2010), Proceedings, 21-24 July 2010, Bregenz, Austria (2010) `https://goo.gl/lbSJfE`
50. G. Brennan and P. Pettit: Unveiling the Vote. British Journal of Political Science, vol. 20, no. 3, pp 311-333 (1990) `http://goo.gl/kgQT22`
51. J. Heckleman: The Secret Ballot Protects the Incumbency Advantage. The Independent Review, vol. 8, no. 3, pp. 419-425 (2004) `http://users.wfu.edu/heckeljc/papers/published/IR.pdf`
52. J. Heckelman: The Effect of the Secret Ballot on Voter Turnout Rates. Public Choice, vol. 82, pp. 107-124 (1995) `http://users.wfu.edu/heckeljc/papers/published/PC1995.pdf`