Framing Electoral Transparency: A Comparative Analysis of Three E-vote Counting Ceremonies

Olivier Bélanger*[1], Randi Markussen†[1], Lorena Ronquillo‡[2] and Carsten Schürmann§[1]

[1]DemTech, IT University of Copenhagen, Denmark
[2]Copenhagen School of Design and Technology, KEA, Denmark

This paper takes up the question of transparency in electronically enabled elections (e-voting). The principle of transparency is central to electoral governance as it provides means for electoral stakeholders to observe and ensure the integrity of an election. However, the issue of transparency in the field of e-voting has been proved to be difficult to tackle practically as well as analytically. In this paper we introduce the notion of 'frames of transparency' and deploy it to conduct a comparative analysis of three e-vote counting ceremonies in Norway, Estonia and Australia. We ask the question of how transparency is framed during these ceremonies, that is what features of the electronic votes counting process are made visible and what others are omitted. Our analysis reveals that e-voting ceremonies emphasizes bureaucratic and technocratic frames of transparency, while the democratic frame is the most difficult to uphold.

1 Introduction

Today, electoral management bodies (EMBs) around the world increasingly use information and communication technologies to support the administration of elections (OSCE, 2013a). These technologies range from the use of basic tools such as word processing

*obla@itu.dk
†randi@demtech.dk
‡lorr@kea.dk
§carsten@demtech.dk

and spreadsheets to more complex data processing tools such as database management systems, optical scanners and Internet voting. Electoral technologies provide EMBs with new capabilities, but also pose democratic challenges. Contrary to the conventional pens and paper, the inner workings of computers are not visible to the 'naked eye' (OSCE, 2013a). The inherent opacity of e-voting systems is problematic since confidence in the result of an election is based on the premise that all aspects of an election should be transparent. Transparency is critical for the public examination and control of elections which is fundamental in democratic elections.

During the last decade, the election community has struggled to formulate policies to guide national efforts to digitalize electoral processes. The notion of transparency should be instrumental in this. Different mechanisms have been devised to improve electoral transparency in e-voting systems such as testing, auditing and certification of the voting technologies. However, we argue that understanding transparency is critical to deal with the broad democratic challenges involved in e-voting. Of special interest to us are in this regard e-vote counting ceremonies, such as those that were organized in Norway, Estonia and Australia designed to make some aspects of the decryption and counting of e-votes visible to a public.

In this paper we first examine how e-voting systems are challenging electoral transparency by identifying three forms of opacity. We do this by looking into the resources about e-voting produced by international election observation organizations and intergovernmental organizations such as the Council of Europe. In order to investigate transparency further we offer three distinct ways of analyzing transparency, which we conceptualize under the notion of frames of transparency: (1) bureaucratic framing: transparency as rule-governed elections; (2) technocratic framing: transparency that stems from the verification of technical aspects of e-voting systems; and (3) democratic framing: transparency stemming from the direct observation of electoral activities and public involvement. Based on this typology we analyze, compare and discuss three e-votes counting ceremonies held in Norway, Estonia and Australia.

2 E-Voting and the Problem of Opacity

The increasing use of electronic voting technologies in elections is recognized by the international election observation community as a new major challenge facing electoral transparency (The Carter Center, 2007). In any e-voting system, there is an inherent tension between the ability to convince the public about the integrity of the election while protecting the secrecy of the vote. How can the public and election observers gain confidence in the outcome of the election when steps such as testing, set-up of the system, conduct of voting, counting or destruction of the data are black-boxed? Our review of the literature of the international election observation community reveals that e-voting systems pose, in their views, three main problems to electoral transparency: (1) the problem of observability; (2) the problem of understandability; and (3) the problem of corporate secrecy.

First, the obvious issue is that e-voting systems are not easily observed with the

naked eye of an observer. This is what we call the problem of observability. The paper ballot system, which consists of people, pens and paper, is transparent as in paper-based systems, election observers may watch ballots being issued, voters placing their ballots in the ballot box and ballots being counted. In comparison, electronic voting systems include numerous elements that are not directly observable. The counting of ballots, just to give an example, is not anymore conducted manually by hundreds of citizens volunteers, which are in principle, easily observable by the eye of an observer, but by a group of a few technical experts operating computers.

Beyond 'visibility' matters, another challenge to electoral transparency stems from the complexity introduced by e-voting systems and the capacity of the observer to understand the functioning of the system. This is what we call the problem of understandability. Given that the voting channel is based on computer technologies, electronic voting technologies are often considered 'black boxes' which non specialist observers are neither able to observe nor understand the inner workings of. Instead, the inherent complexities can only be understood (and often only in part) by few experts, which means that the integrity of the electoral process relies largely on the expertise and experience of this small group in contrast to thousands of poll workers (International IDEA, 2012). There is also mention of a widening gap between the knowledge of the technicians who run the election and that of the electorate and political parties (The Carter Center, 2007). The gap, it is feared, can grow so wide that it risks to erode the general public capacity to lodge complaints or legal challenges. In the case of the counting of e-votes, only a very few people observing such a process understand the technical aspects of cleansing, mixing and decrypting an electronic ballot box.

Finally, proprietary concerns are also challenging electoral transparency. Trade secrets, proprietary code and non-disclosure agreements are at odds with the idea of transparent elections. IT vendors intentionally make their solutions proprietary arguing for the need to protect their trade secrets in order to keep their competitive advantage (Maurer and Barrat, 2015). The problem of propriety concerns not so much the counting stage of an e-enabled election, but it is imminently problematic during the testing stage where expert observers are either prevented to access the e-voting system in order to assess it or are submitted to non-disclosure agreements, which forbid them to make the results of their investigation publicly available. The reason why many countries admit proprietary systems in the electoral process is due to the legal framework not explicitly ruling this out. A notable exception is Germany, where the Supreme Court has ruled an election law unconstitutional because it did not guarantee sufficient provisions to keep procured technologies transparent.

These different forms of opacity introduced by e-voting systems raise questions such as: What can and should be visible in e-voting systems? What kind of access to the e-voting processes is needed by observers? How can one make transparent the workings of e-voting systems where the processes of counting and tabulation are invisible? What steps are actually taken by electoral management bodies to promote transparency? How do experts verify the system and communicate the results to the public? How can the public be involved in the electoral process in a meaningful way? We see the emergence of e-vote counting ceremonies as a partial answer to these questions. In the following section,

we introduce our approach for investigating electoral transparency in the ceremonies by introducing the notion of 'frames of transparency'.

3 Investigating Electoral Transparency

Despite its omnipresence across the election literature, there is no conceptual framework that describes how electoral transparency is achieved. What we find instead is a set of heterogenous mechanisms, measures, recommendations and best practices promoting electoral transparency. For example, the Council of Europe suggests that transparency is "the concept of determining how and why information is conveyed through various means" (Council of Europe, 2011). For the International Foundation for Electoral Systems (IFES), electoral transparency is "the term for a clear and open process, which is understandable and accountable to the electorate" (Kaplan, 2002). These examples reveal how transparency is often casually defined leaving much left to an assumed tacit understanding.

No doubt transparency is an extremely difficult notion to tackle practically as well as analytically. In our view transparency is not an object that can be 'looked at' and examined. Rather, it is a dynamic and instrumental notion in the name of which selected aspects of the electoral process are made visible in order to uphold trust in the integrity of the results. That being said, we believe that it is possible by synthesizing election observation sources to investigate at a conceptual level attempts to make certain aspects of an election transparent. Our goal is to make explicit common tendencies in the use of the word transparency in the election community and to suggest three different ways of understanding it. To this end, we develop a framework that conceptualizes transparency as a practical achievement by introducing the notion of frames of transparency.

In order to provide a view of transparency that emphasizes its democratic potentials, we propose the notion of 'frames of transparency'. The notion of frames is an empirically useful concept to describe how concerns about electoral transparency are dealt with by different means. According to a well-known definition, the notion of 'frame' refers to 'ideas' and 'values' that help to 'select some aspects of a perceived reality and make them more salient in a communicating context' (Entman, 1993). In framing electoral transparency, one selects some features of the electoral process to make them more noticeable, meaningful or memorable while omitting some others. We argue that the notion of framing offers a way to describe the democratic aspects of electoral events such as the e-vote counting ceremony.

Electoral transparency is the effect of the interaction between different aspects of an election and the observer's capacity to observe and understand them. A feature of the electoral process emphasized in a context such as the e-vote counting ceremonies can be difficult for observers to notice, interpret, or remember because of their pre-existing (or lack thereof) knowledge about the procedures and technical aspects of e-voting systems. For instance, as we will see below, the numerous technical aspects emphasized during the e-voting ceremonies were, to some extent, only transparent for a small group of experts.

By reviewing sources from election observation organisations and intergovernmental

bodies, we propose three ways of framing transparency. First, the bureaucratic frame of transparency emphasizes the importance of designing clear rules and procedures governing the electoral process. Second, the technocratic frame of transparency emphasizes the importance of making the inner workings of an e-voting system knowable through observations, tests, audits and certifications. Finally, the democratic frame of transparency emphasizes the importance of giving direct access to electoral activities to a wide range of election stakeholders (beyond civil servants and technical experts), but in particular to the citizens, scrutineers, parties, not only to directly observe electoral activities, but also to actively take part in them. Both the bureaucratic and the technocratic framing are important from a democratic point of view, of course. They are constitutive in how contemporary governance takes place in most countries. They do not, however, highlight how citizens and in the case of voters more explicitly participate in the governance process, an aspect that is particularly important in democratic elections.

3.1 Bureaucratic frame: Transparency as rule-governed electoral process

One frame of transparency emerging from the election literature is that the state shall be open about the rules and procedures governing the electoral process. According to the OSCE, "[t]he principle of transparency requires that the election be carried out according to due process of the law, and according to legal ground rules that are established in an inclusive and open manner" (OSCE, 1999). Attempts to strengthen electoral governance have strongly focused on the design of electoral systems based on accessible and well defined rules, see e.g. (Massicotte et al., 2004; Norris, 2004). In fact, governance according to fixed and published rules is perhaps the most common frame of transparency, which requires that information and procedures that are accessible to the public (Hood and Heald, 2006).

This frame of transparency comprises typical electoral procedures such as the notification of elections, registration procedures, nomination of candidates, the voting procedure, publishing and explaining the procedures for complaints about the electoral process (Council of Europe, 2011), but also procedures that are a direct result of using e-voting systems. The OSCE asks its member states, for instance, to consider if their respective legal framework takes into account the implications of new technologies, including adequate provision for access of observers, system audits, as well as the possibility for recounts, mandatory audits of results and legal challenges to election results (OSCE, 2013a). Along similar lines, International IDEA insists that rules and procedures governing the procurement process of e-voting systems are essential to avoid the impression that the process appears hijacked by vendors (International IDEA, 2012). The criteria used for selecting any e-voting system should be made clear and publicly available in advance. The Council of Europe (CoE) also recommends the development of procedures defining which stakeholders shall have access to what and when (Council of Europe, 2011).

Transparency of the different electoral procedures is said to contribute to the voters' knowledge and understanding, thereby generating trust and confidence among the general public (Council of Europe, 2010). The notion of a neutral, independent process

upholds one version of electoral governance that is transparent.

3.2 Technocratic frame: Transparency as control of technical aspects

A second frame of transparency, which emerged from the introduction of e-voting systems, aims to make the internal workings of the systems used within an election knowable. As we have seen, e-voting systems pose special challenges to observers, due to the different levels of opacity of the technical components.

This frame of transparency includes mechanisms such as audits, impartial and independent certification, and testing, which are all said to promote electoral transparency (The Carter Center, 2007). The CoE suggests, for instance, electoral management bodies to provide observers with an opportunity "to have access to relevant software information, to see physical and electronic safety measures for servers, to inspect and test certified devices, to have access to and test sites and information provided for remote e-voting, and to observe cast electronic votes entering the electronic ballot box and that votes are being counted" (Council of Europe, 2004). It is also suggested that the software used in e-voting systems should be subject to impartial inspection by an independant body (The Carter Center, 2007). The CoE advises its member states to audit the voting software source code, the configuration as well as all hardware and software components of the e-voting system by an independent organization (Council of Europe, 2011).

It is worth mentioning that these mechanisms of transparency transfer the responsibility of overseeing the electoral process from the general public to a community of experts, see e.g. (Barrat, 2012). If permitted by the contract, election commissions often make the findings of third-party audits available, we note, however, that alongside the public is left with only diminished abilities to challenge any part of the electoral process.

3.3 Democratic frame: Transparency as observation and participation in electoral activities

A third frame of transparency advocated by the election community is emphasizing directly observable electoral activities. This is illustrated for example in the second part of the OSCE's definition of transparency, which emphasizes this dimension: "A transparent process limits the possibility for election fraud, and thus the vote count should be visible and verifiable from the level of the polling station, to any intermediate levels of the election administration, and finally to the national election authority" (OSCE, 1999). In conventional elections, numerous arrangements emphasize transparency including the invitation for anyone to become an election official. In many western countries, it is common practice to allow teams consisting of delegates with different political backgrounds to inspect and control the electoral processes.

One aspect of this framing promotes transparency as the direct observation of electoral activities. The CoE suggests that its member states should ease the presence of observers in polling stations and/or data transfer and data processing sites (Council of Europe, 2011). The OSCE observes that not all aspects of e-voting systems can be directly observed. However, a number of activities can be open to observers, such as

the deployment, setup and modification of the system by administrators and vendors, but also the activities of certification, testing, and audit authorities (OSCE, 2013a). Opening decision-making to observers is considered to contribute to electoral transparency (Council of Europe, 2010). The e-vote counting ceremonies analyzed below are also contributing to this form of transparency.

That being said, we would like to suggest that the involvement of the public in electoral activities should also be included in the democratic framing of transparency. Our argument here is that transparency is not solely achieved by giving the citizens the right to observe election processes, but also by giving them the right to participate in them. The distributed counting in paper-based elections, for example, relies on the participation of people, their collaboration and their ability to control one another. This creates electoral transparency.

Also, from a democratic perspective, the main weakness of any e-voting system consists in the difficulty for average citizens to conduct their own verification (Barrat, 2012). To answer this problem, the election community has been advocating the use of software independent voting systems. "A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome" (Rivest, 2008). One way to achieve software independence is via a voter-verified paper audit trail, that enables the voter to ensure that his or her intent was correctly recorded. The CoE has integrated software independence in its own recommendation requiring that e-voting machines shall produce a physical interpretation of the vote in order for the voter to verify its correctness, for the auditor to conduct, for example, a risk-limiting audit (Council of Europe, 2011; Stark, 2010). An e-voting system can be end-to-end verifiable, which means that it produces enough evidence for anyone to participate in checking this evidence for achieving high levels of confidence that the overall result of the election is correct.

4 Case Studies

In the case of e-enabled elections where the counting of votes is impossible to observe by conventional means, we see e-vote counting ceremonies as emergent communication events in the electoral cycle created by electoral management bodies to mitigate the opacity introduced by e-voting systems. An e-vote counting ceremony is a public event, generally performed in front of an audience, witnessing and following the process by which electronic votes are officially decrypted, counted and the election results are ultimately published. This event is meant to make the decryption and counting processes visible and generate trust about the integrity of the election result.

Even though the list of countries having engaged in electronic elections has in general been increasing, not all countries have offered such processes as a public event. To our knowledge, only three countries have done so: Norway in 2011 and in its last parliamentary election in 2013, Estonia from 2007, and the State of Victoria, in Australia, in its last election in 2015. The nature of such an event, though, differs from country to country, and even from election to election. Some of these ceremonies have been addressed

to a mixed public, while some others were more addressed to experts. In some cases, the event was made available online or even lived streamed, while some others could only be witnessed by people being present and/or personally invited to the event. Here we analyze the three e-vote counting ceremonies, held in Norway, 2013, State of Victoria 2014, and Estonia, 2015, and we report our observations regarding how the different ceremonies are framing electoral transparency.

4.1 Decryption and Counting Ceremony in Norway 2013

The Decryption and Counting Ceremony of the Norwegian Internet voting pilot took place on election day September 9th, 2013 in an auditorium in the Ministry, two hours before the election closed. The audience consisted of election observers from many different countries who had attended a seminar on the Norwegian electoral process held in the same building on the 8-9th of September, and included representatives from the OSCE, Carter Center, representatives of various election commissions, scientists, vendors, and researchers. The ceremony was simultaneously translated into English and, just as importantly, open for all citizens. The event was also broadcast on the Ministry's homepage. The host, Christian Bull, head of security of the voting project, explained the different aspects of internet elections and guided the audience through the ceremony. The purpose of the ceremony was to decrypt and tally the electronic ballot box that had been retrieved from the central database server some time before the event, in the presence of the verification team and the observers.

4.1.1 Bureaucratic framing of transparency

The Norwegian Election Act allows electoral pilot projects. Based on the Council of Europe's recommendations, this pilot was governed by regulations issued by the Ministry. Different from the September 2009 pilot, this time an Internet Election Committee (IEC) was appointed to ensure that the Internet voting pilot was conducted in accordance with these regulations in a manner that was open and the voters could trust (Ministry of Local Government and Regional Development, Norway, 2013). The IEC was an independent body that was tasked to supervise the preparation, verification and approval of the results. They also had the authority to suspend or cancel the pilot in case of irregularities. The IEC consisted of nine members covering technical and political competences as well as representatives of the municipalities involved in the pilot. The OSCE report puts an emphasis on this by recommending that more rules and procedures on how people are elected to the IEC are made explicit in order to avoid conflict of interest and secure independence of the team (OSCE, 2013b). Another task of the IEC was to appoint an independent verification team to check the evidence generated by the decryption and counting process (OSCE, 2013b). The creation of the IEC and the legal framework anchor the pilot within the bureaucratic framing. The legal framework was described in detail during the workshop preceding the ceremony.

4.1.2 Technocratic framing of transparency

The organizers of the Norwegian e-vote counting ceremony spared no cost to make the decryption and counting visible and transparent from a technical point of view. Two assistants were executing the three phases (cleansing, mixing and e-counting) using one dedicated laptop each, that were placed on a large table on the auditorium stage. In addition, three overhead screens displayed various aspects of the process: one screen was showing a diagram giving an overview of the technical setup; a second one (the technical screen) was showing the Linux prompt where the assistants were typing various commands; and a third one described the respective phases of the process and depicted the command that had to be executed. Furthermore, a safety deposit box that contained a second, smaller safety deposit box that in turn contained the USB key with the election data was placed in one corner of the room while a blender was placed in another corner. This blender would be used to destroy USB sticks containing information that would otherwise link the voter to his or her vote.

During the ceremony, the organizers deliberately gave the audience a glimpse into the inner workings of the decryption and counting process like, for instance, which folders were accessed, what their content was, etc.

The organizers also made great efforts to convince the audience that the data weren't tampered with through the different phases of the ceremony. To make visible that the three laptops were air-gapped, the organizers color-coded the cables connecting the laptops to the different servers and the transfer of data from one laptop (phase) to the next one, was always done by means of USB sticks. These USB sticks were taken from the inner safety deposit box, for which the verifier team held the physical key. Before each use, the organizers also demonstrated that the memory sticks were new by showing on one screen their content, so that everyone could check that they were empty. Furthermore, in order to show that the cleansed ballot box and the mixed ballot box remained unchanged when transferred from one phase to the other, and no process injected new votes into the ballot box, a well-known cryptographic tool known as hash function was used. The output of a hash function is unique (at least for our purposes it may be considered as such), thus it was used here to prove the equality of two files located in different machines. In the context of the ceremony, the hash value of the file to be transferred was shown both before being copied to the memory stick, and after being copied to the next machine. This enabled the verifier team, as well as anyone among the audience, to take a picture of the first hash value and compare it to the second one for equality. Because of the sensitive nature of the data contained in the memory sticks used between the cleansing and the mixing and between the mixing and the e-counting phases, as well as to illustrate that the ballots in these memory sticks should never be recovered, these memory sticks were immediately destroyed in the blender after use.

Once the mixing phase was completed, the verifier team received two USB sticks containing, respectively, the mixed ballot box and the zero-knowledge proofs generated during the mixing phase, to check that the mixing had been conducted correctly. Later on, the host declared that the verifiers had informed him that their checking was successful.

Prior to the election, the organizers created a private election key, shares of which were given to each IEC member on a smartcard. Six out of the nine shares were needed to reconstruct the key necessary to decrypt the e-votes (Kommunal og Regionaldepartamentet, 2013). During the counting phase, the host selected those six IEC members at random, and once the private election key was retrieved, they decrypted the e-votes and thus obtained the election results. These results were then copied to a USB stick, which would be transferred to the election information system (EVA) after the ceremony. Finally, the verifier team received the USB sticks containing the mixed ballot box and the zero-knowledge proofs generated in the e-counting phase, to check the decryption.

4.1.3 Democratic framing of transparency

The Norwegian e-vote counting ceremony was an attempt to mitigate the inherent opacity introduced by e-voting systems also by making public the counting of e-votes. Mechanisms were deployed in order to involve a broad set of electoral stakeholders in the counting stage of the Internet voting process, thus emphasizing the democratic framing of transparency. The ceremony itself can be understood as a transparency mechanism affording the public to 'directly' observe the counting of e-votes. But more than that, the formation of the IEC, which was created having plurality in mind by delegating responsibilities between politicians, independent experts and local administrations, reflected the ideal of a direct participation in the electoral process. During the ceremony, the host involved the audience to determine the order at random in which the members of the IEC would present their USB keys to reconstruct the private election key. The live broadcast of the event on the Internet and its publication afterwards is another such mechanism. During the ceremony, media entered the room to broadcast live the event on national news.

4.2 E-vote counting ceremony in Estonia 2015

Estonia was one of the first countries to offer Internet voting as an alternative voting channel to all eligible voters in national elections. The election of 2015 was their third parliamentary election. The e-vote counting ceremony took place on the evening of election day, 1st March 2015 in the conference hall of the parliament, the Toompea Castle, in Tallinn. The audience was composed of, and in no particular order, the media, political parties representatives, researchers, members of foreign electoral management bodies, representants from other IT vendors and domestic and international observers including an Election Expert Team from the OSCE consisting of three experts. The ceremony was held in Estonian and simultaneously translated into English.

4.2.1 Bureaucratic framing of transparency

In Estonia, the conduct of parliamentary elections is regulated by the 1992 Constitution and the 2002 Riigikogu Election Act. In 2012, following the recommendation of the OSCE, a number of amendments were introduced to the Election Act to further regulate and consolidate aspects of Internet voting (OSCE, 2015). One amendment of interest to

our analysis regulates the formation of the Electronic Voting Committee (EVC), under the auspices of the National Electoral Committee (NEC). This committee is responsible of organizing Internet voting, verifying the electronic voting results and has the authority to suspend or cancel the Internet election in case of irregularities. The committee was composed of seven members appointed by the NEC from among experts in relevant technical disciplines, such as Internet security, computer programming, and administration of servers (OSCE, 2015). Another amendment made to the Election Act in 2012 describes in great detail the procedures governing the counts of electronic ballots, and by extension the sequence of events taking place during the e-vote counting ceremony. The provision specifies, among other things, that the EVC shall verify the results of e-voting on election day after 7 p.m.; that at least one half of the members of the EVC and the NEC shall be present at the counting of votes; that the NEC shall open the e-votes using the private election key; that the counting of e-votes shall be public; that the voting results shall not be disclosed before 8 p.m. and; that the chairman of the EVC shall enter the voting results in the election information system immediately (Riigikogu Election Act, chapter 9, paragraph 60: Counting of votes cast using electronic means).

These different amendments to the Election Act regulating the counting ceremony are essential to the bureaucratic framing of transparency. These rules, discussed and made publicly available, are the legal/formal 'backbone' of the ceremony dictating its rhythm and the sequence of the events that we observed. These rules were made explicitly visible during the workshop held before the ceremony, but not during the ceremony itself.

4.2.2 Technocratic framing of transparency

The organizers of the Estonian ceremony put great emphasis on the technical aspects of the counting of e-votes. The setup of the conference hall, for instance, was designed to foreground and make visible the devices used during the Internet election and, to some extent, their inner workings. On stage, there were two overhead screens and three devices arranged on a long table: (1) the server containing the electronic ballot box; (2) the server used to count the ballots and; (3) the hardware security module (HSM) containing the private election key necessary to decrypt e-votes. The devices were connected to a computer screen, a keyboard and a projector. While the central overhead screen was showing explanatory slides accompanying the counting process, the smaller screen, which we will call the technical screen, located to the lower right of the main screen displayed a menu in Estonian from which a member of the EVC selected the next action to be executed. It also displayed the commands executed on the servers and their responses. Most of them were Linux commands, and as in Norway, no graphical user interface was used.

Beyond the setup of the room, we noticed that the organizers paid special attention to making visible and trustworthy the integrity and the secrecy of the e-votes while they were being moved from one medium to another. For instance, when the organizers transferred the encrypted votes from the server storing the ballots to the counting server, they burned the data on a green CD and made its content (2 files) visible on the technical screen. In addition, the organizers checked the integrity of the data by computing, as in

Norway, a hash value for each file that demonstrated that the transfer did not corrupted the files. The operator then transferred the encrypted e-votes to the counting server connected to the HSM. In order to decrypt the votes, the EVC members needed to unlock the HSM. The particular unlocking scheme used here required that at least four of the seven EVC members presented their respective key shares to the HSM. The four members of the EVC stepped forward, presented their shares to the HSM, and the decryption process began. Note that this makes visible that it will take four or more EVC members to collude in order to break the secrecy of the vote. The result of the decryption process were burned onto a yellow CD, transferred to the election administration system, and checked for integrity. The audience could follow the procedure on the main screen. Lastly, the deputy chairman of the EVC displayed the final results of tallying all Internet votes.

4.2.3 Democratic framing of transparency

The purpose of the ceremony was to make public the decryption and counting of the e-votes as well as the publishing of the final results of the Internet elections. In the light of the democratic framing, the ceremony itself can be seen as a singular event contributing to the overall transparency of Internet elections by enabling multiple stakeholders to observe 'directly' the decryption, counting and publishing of e-votes. The ceremony was open to everyone who registered as an observer, local or international, who were expected to participate in a seminar on the Estonian electoral system the day before. The ceremony was neither broadcast nor published on the Internet afterwards. We argue that the seminar contributed to a democratic framing of transparency. During the ceremony however, there was very little interaction between the EVC and the audience.

4.3 Mixing and Decryption Ceremony in Victoria in Australia 2014

Our final case study is that of the decryption ceremony of the Victoria State Election on November 30, 2014 that took place in the back office of the Victoria Electoral Commission (VEC) at 530 Collins Street in downtown Melbourne. The ceremony was organized by Craig Burton, the program manager of the vVote project, a voting system that was custom-made for the elections in Victoria. Participation was by invitation only. Present at the ceremony were mainly scientists, implementers, reviewers, deputy commissioner and election officials but neither election observation missions nor scrutineers. Even though some countries outside of Europe, as for instance the US, are members of OSCE, Australia is not. Australia does in general not permit election observation by foreign organizations. The ceremony was videotaped (by us and not the organizers), which is available on Youtube.[1]

The goal of the ceremony was not as much to convince the audience that the results of the mixing and decryption were correct, but more a demonstration about how the vVote voting system works at all. In fact, the ceremony that we, the audience, experienced was only a repetition of what took place behind closed door the night before at the

[1] `https://www.youtube.com/watch?v=I5GId7K-Zl8&feature=youtu.be`

same location. The vVote system is the custom-built kiosk-based voting solution that is loosely based on Prêt-à-Voter (Ryan et al., 2009) and implemented by Steve Schneider and his team at the University of Surrey. vVote's hallmark characteristics is that it is end-to-end voter verifiable, which means that each voter can check after the election, (1) that their encrypted ballots were recorded as intended, (2) that the mixing of all ballots was successful, (3) that all ballots were correctly decrypted, and (4) that the resulting election result was correct. It is noteworthy to emphasize that the ceremony was held as part of a binding pilot of limited scope. The VEC had authorized that vVote only be used in selected polling stations in Victoria by people with disabilities and those with special language needs and for all voters living abroad in London, United Kingdom. Although the system was designed to handle a million votes, only 1121 ballots were collected during the advance voting period, which was the only period during which the system was authorized to be used. During the ceremony these 1121 e-votes were mixed, decrypted, printed, and inserted into the manual count (Burton et al., 2015).

The ceremony took place in the office space adjacent to a server room of the VEC. Four laptops, programmed to execute the mixing and decryption programs, and a desktop computer, programmed to serve as the central node that would distribute the work among the laptops and interpret the results, were placed next to each other on a desk. The audience was in part sitting and in part standing in front of this desk. Burton led the ceremony using simple instructional and rhetoric devices, such as ballot papers, receipts, etc. to explain the process, how it is started, what was happening, and what happened after the decryption. During the ceremony, the audience could follow the individual steps, but at no time during the ceremony was the result made visible.

4.3.1 Bureaucratic framing of transparency

Only little can be said about the bureaucratic framing of transparency. The Electoral Act 2002, No. 23 of 2002 Part 6A -Electronic Voting, paragraph 110E (2) f) requires that "the computer program can produce a paper record of each vote cast using an electronic ballot-paper to enable the counting of votes in the election." Details of the ceremony that surround the production of the paper record of each vote are not specified in the legislation. This means, that the VEC was not obliged to hold such a ceremony and thus not bound to any specific rules on how to organize it. On the other hand, the individual steps of the interaction between the program manager and the vVote system were well explained and could easily be followed. When the audience arrived, the desktop computer was already prepared with a digital ballot box. No evidence was given that the ballot box that would be decrypted was indeed the real ballot box. The mixing and decryption procedure was initiated by the program manager and consisted of (1) the launching of the mixing and decryption software on each laptop computer, (2) initiating the main program on the desktop computer, and (3) retrieving the comma separated values (CSV) file from the main computer. This CSV file contained the preference from all decrypted ballots and it was printed to produce paper evidence that would be inserted into the manual count. It should be mentioned that the audience was not informed about the larger legal framework; the ambition of the ceremony was to achieve technocratic

and not bureaucratic transparency.

4.3.2 Technocratic framing of transparency

As the vVote system is end-to-end verifiable, the authenticity of the CSV file can be - by the virtue of a proof of knowledge - established by checking the additional evidence that was published post election on the internet. End-to-end verifiable systems are designed to verify the election result and not the process that computed it. This means that the mixing and decryption ceremony is not strictly necessary for trust generation, but it contributes to a large extent to the technological understanding of the electorate, if done right. We notice that the program manager focused the ceremony on explaining how the vVote system works in general. During his 20 minutes presentation, the program manager explained the technicalities underlying the vVote system, for example, that voters received a randomized version of the ballot with a 2D barcode when registering to vote, that the barcode encrypts the permutation of the voting options and can be used to decrypt a ballot, and that the ballot itself is a list of numbers in clear text, just not in the right order. He explained the idea behind cryptographically mixing the ballots, and executed the mix on a network of the four aforementioned laptops. Although his presentation was to a large degree independent of the ongoing election and the result, it made it clear, how the process worked, and, perhaps more importantly, it was an invitation to check the published proofs of knowledge once they were published on the web bulletin board. Burton's presentation of the protocol, together with the availability of the source code (everything is published on Bitbucket), alleviated the problem of observability, as the audience was left with the impression that vVote is all mathematics and implementation, but it also exposed the tremendous complexity behind the vVote system. Without acknowledging any of the residual trust assumptions, the ceremony made clear that by design all important parts of the process are voter-verifiable.

4.3.3 Democratic framing of transparency

This decryption ceremony is best described as an early pilot or a proof of concept. This means it was not designed to cater to a bigger audience and certainly not to create confidence in the overall election result. But with the democratic framing in mind, it is exactly here where tremendous opportunities in terms of public trust generation and public involvement lie. End-to-end verifiable systems depend critically on public participation and the public checking of cryptographic evidence. Thus, one idea is that instead of planning a ceremony to explain the process only to a small group of experts, future editions could explicitly invite scrutineers, stakeholders and press to teach them about the basic principles of vVote, and to trigger voter verification of the evidence produced by the system. In Victoria, it is common practice to celebrate democracy and the election together on Federation Square in downtown Melbourne, where hundreds of citizen assemble to listen together to the latest prognosis. In 2014, in parallel to this festival of democracy, the digital votes were mixed and decrypted behind closed doors. From what was experienced during the ceremony, it is easy to imagine other

innovative ways on how the ceremony could have also been integrated into the celebration of democracy that was happening on Federation Square. In summary, the mixing and decryption ceremony organized by VEC has the potential to contribute to a democratic framing of transparency.

5 Discussion

We argue that our conceptual framework captures the different ways in which transparency can practically be achieved. The different 'frames of transparency' articulate how different set of features of the electoral process are emphasized. Here, we compare the different ceremonies and discuss our findings.

In the light of the bureaucratic framing, we observe that e-voting systems call for additional regulations and structures to organize and control e-enabled elections. The bureaucratic framing contributes to electoral transparency by providing and making accessible to a public a clear set of rules, which contribute to build trust in the electoral system. As we have seen, Norway and Estonia went a long way to regulate and consolidate critical aspects of their respective e-voting systems in their legal framework. These new regulations not only govern e-voting, but also, at least in the case of Estonia, determined the structure of the e-vote counting ceremony. Furthermore, both countries formed committees dedicated to the organization and administration of Internet voting. In Estonia, the committee was put in charge to prepare, organize, and determine the result of the Internet election while in Norway the committee had much fewer responsibilities but still played a central role during the ceremony. Victoria's ceremony, on the other hand, was not subject to a specific regulatory framework, as far as we could discern.

The technocratic framing helps us to underline how the technical aspects, such as cleansing, mixing, decryption, counting, and publishing of the results, were foregrounded during the ceremonies. In Norway and Estonia for example, dedicated overhead screens (the technical screens) were displaying the command lines executed during the ceremony and the response of the devices used for e-voting, whether they were the servers that collected the e-votes or counting servers. We claim, however, that this framing addresses inherently IT experts and selects a public that is knowledgeable in technical matters. As far as we understand it, the three ceremonies were organized exclusively by computer scientists (as opposed to civil servants with a legal training) who draw on their particular background. The efforts they made to demonstrate the process by making technical and black-boxed and complex procedures visible are significant, but of little help for members of the audience without an IT background. From the perspective of the technocratic framing, an important question is to what extent the event convinces the expert community, and to what extent other people understand the technical aspects in the ceremony and fulfill their role as free and informed citizens.

At last, the democratic framing of transparency is greatly challenged by the introduction of e-voting systems. These ceremonies bear witness to how the role of the public in elections is under transformation. The idea of representing the public by proxy

increasingly appear in the discussions of election observation and intergovernmental organizations (Barrat, 2012), as well as their expertise seem to play a more dominant role in overlooking elections and securing the integrity and the legitimacy of an election measured by their own standards. When compared to conventional votes counting processes, it is obvious that the ceremonies makes certain assumptions regarding the public that are hardly apparent within the bureaucratic and technocratic framing, but are made visible by the democratic framing. It becomes evident that very few people are in reality participating in the process in the ceremony and in the Internet election as a whole. The public in the auditorium are assigned the role of an audience, not as active participant the way people may involve themselves in conventional voting process. The notable exception in Norway was when the audience determined the order in which the members of the IEC presented their USB sticks. Even if the bureaucratic and technocratic framings suggest that we can rely on objective procedures and the assessments of technical experts, the democratic framing makes evident that transparency is not exclusively a question of whether people are knowledgeable, even though this is of course important. Information is important, but we argue that the active involvement of citizens in the counting process has been and should continue to be constitutive of democratic elections.

6 Conclusion

This paper describes how the introduction of e-voting systems furthers and exacerbates the delegation of the control of the electoral process from the public and the civil servants to a small group of technical experts. Our depiction of three e-vote counting ceremonies reveal an overall tendency of mainly framing transparency in technocratic terms, that is by emphasizing the technical aspects of the respective decryption and counting processes. The dominance of the technocratic framing comes mostly at the expense of democratic and to a somewhat lesser extent of the bureaucratic framing and bears witness to a deep transformation of the electoral process. This begs to question to what extent is it possible to re-involve the public in e-enabled electoral processes? In their current form, the ceremonies are designed to cater to a passive audience. However, despite their actual technocratic bias, we see potential in these ceremonies to re-involve the participation of the public in the electoral process. In this regard, the most advanced ceremony was that organized in Victoria, which could be seen as an encouragement for the public to check their receipts and other published evidence after the official results were published. Furthermore, we remark that none of the ceremonies attempted to make explicit the residual trust assumptions that the public has to take for granted in order to believe the published result.

In this paper we discussed only decryption and counting ceremonies. However, there are other ceremonies that could be studied as well: a ceremony for creating verifiable randomness, a ceremony for creating digital ballot forms (if applicable), or a ceremony for creating and distributing shares of the private election key among the internet voting committees, to name a few. We believe that our conceptual framework of transparency

can also be applied here. In particular it would be interesting to study the role of Benaloh challenges (Benaloh, 2006) in empowering a voter to participate in the election activities by challenging the validity of a digital ballot using the democratic frame of transparency.

Acknowledgements

The authors were supported in part by the DemTech grant 10-092309 from the Danish Council for Strategic Research, Program Commission on Strategic Growth Technologies.

References

J. Barrat. Observing e-enabled elections: How to implement regional electoral standards. International IDEA, Stockholm, Sweden, 2012.

J. Benaloh. Simple verifiable elections. In *2006 USENIX/ACCURATE Electronic Voting Technology Workshop, EVT'06*, Vancouver, BC, Canada, August 2006.

C. Burton, C. Culnane, and S. Schneider. Secure and verifiable electronic voting in practice: the use of vvote in the victorian state election. *CoRR*, abs/1504.07098, 2015.

Council of Europe. Recommendation rec(2004)11 on legal, operational and technical standards for e-voting. Strasbourg, France, September 2004.

Council of Europe. E-voting handbook. Strasbourg, France, November 2010.

Council of Europe. Guidelines on transparency of e-enabled elections. Strasbourg, France, February 2011.

R. M. Entman. Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4):51–58, 1993.

C. Hood and D. Heald. *Transparency: The Key to Better Governance?* Proceedings of the British Academy. OUP/British Academy, 2006.

International IDEA. Introducing electronic voting: Essential considerations. Stockholm, Sweden, 2012.

C. A. Kaplan. A guide to transparency in election administration. IFES International Foundation for Election Systems, Washington, D.C., 2002.

Kommunal og Regionaldepartamentet. Regulations relating to trial internet voting during advance voting and use of electronic electoral rolls at polling stations on election day during the 2013 parliamentary election in selected municipalities, June 19 2013.

L. Massicotte, A. Blais, and A. Yoshinaka. *Establishing the Rules of the Game: Election Laws in Democracies*. G - Reference,Information and Interdisciplinary Subjects Series. University of Toronto Press, 2004.

A. D. Maurer and J. Barrat. *E-Voting Case Law: A Comparative Analysis*. Ashgate, 2015.

Ministry of Local Government and Regional Development, Norway. Internettvalstyret er oppnemnd. Press release, June 20 2013.

P. Norris. *Electoral Engineering: Voting Rules and Political Behavior*. Cambridge Studies in Comparative Politics. Cambridge University Press, 2004.

OSCE. Election observation handbook. 4th edition. OSCE Office for Democratic Institutions and Human Rights, Warsaw, 1999.

OSCE. Handbook for the observation of new voting technologies. OSCE Office for Democratic Institutions and Human Rights, Warsaw, 2013a.

OSCE. Norway, parliamentary elections, 9 september 2013: Final report. OSCE Office for Democratic Institutions and Human Rights, Warsaw, 2013b.

OSCE. Estonia, parliamentary elections, 1 march 2015: Final report. OSCE Office for Democratic Institutions and Human Rights, Warsaw, 2015.

R. L. Rivest. On the notion of 'software independence' in voting systems. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767, 2008.

P. Y. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia. The Prêt á Voter verifiable election system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

P. B. Stark. Super-simple simultaneous single-ballot risk-limiting audits. In *International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, pages 1–16, 2010.

The Carter Center. Developing a methodology for observing electronic voting. Atlanta, GA, October 2007.