International Experience with E-Voting

Norwegian E-Vote Project

Jordi Barrat i Esteve, Ben Goldsmith and John Turner

June 2012

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS

IFES

25 YEARS

Global Expertise. Local Solutions.
Sustainable Democracy.

International Experience with E-Voting

International Foundation for Electoral Systems
1850 K Street, NW, Fifth Floor
Washington, DC 20006
Email: editor@ifes.org
Fax: 202.350.6701

International Experience with E-voting

Norwegian E-vote Project

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
25 YEARS

Global Expertise. Local Solutions.
Sustainable Democracy.

International Experience with E-voting

Norwegian E-vote Project

Jordi Barrat i Esteve, Ben Goldsmith and John Turner

June 2012

Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the International Foundation for Electoral Systems.

About IFES

The International Foundation for Electoral Systems (IFES) supports citizens' right to participate in free and fair elections. Our independent expertise strengthens electoral systems and builds local capacity to deliver sustainable solutions.

As the global leader in democracy promotion, we advance good governance and democratic rights by:

- Providing technical assistance to election officials
- Empowering the under-represented to participate in the political process
- Applying field-based research to improve the electoral cycle

Since 1987, IFES has worked in over 135 countries – from developing democracies, to mature democracies.

For more information, visit www.IFES.org.

Table of Contents

1. Executive Summary

This assessment report on *International Experiences with E-Voting* has been conducted as part of a larger assessment of the Norway E-Vote Project, a pilot of internet voting during the September 2011 local government elections. This report represents one of seven assessment topics conducted on behalf of the Ministry for Local Government and Rural Development in order to analyze the recent pilot, and determine whether a broader adoption of internet voting would be suitable for future Norwegian elections.

The report largely focuses on internet voting experiences, first reviewing countries which have used internet voting and summarizing their experiences. This review highlights a number of thematic issues and challenges related to internet voting. Four issues are singled out for more detailed analysis:

- Trust in Internet voting
- The secrecy and freedom of the vote
- The accessibility of Internet voting
- The role of stakeholders

The report reviews several examples of Internet voting in more depth, examples where Internet voting has been used for a number of elections – Estonia, France and Switzerland-Geneva. A brief summary of these case studies is presented in the main body of the report, with the full case studies included in the annex. The final part of the report looks at the global experiences of non-remote electronic voting and concludes by identifying emerging trends in the use of non-remote electronic voting worldwide.

Overview of Internet Voting Experiences

The first use of Internet voting for a binding political election was found to be in the U.S. in 2000, with more countries subsequently beginning to trial and use Internet voting. Each year since 2006, four to six countries have used this voting method. A total of 11 countries have now used remote Internet voting for binding political elections of referenda, including Norway. The group of Internet voting system users consists of four core countries which have been using Internet voting over the course of several elections/referenda: Canada, Estonia, France and Switzerland. Estonia is the only country to offer Internet voting to the entire electorate. The remaining seven countries have either just adopted it, are currently piloting Internet voting, have piloted it and not pursued its use, or discontinued its use.

Examples of Internet voting in other countries around the world vary widely in scope and functionality. The early cases of Internet voting were less technically advanced than those being developed more recently. Many of the changes seen in Internet voting systems have been aimed at improving the quality of an election delivered by the Internet voting system and meeting emerging standards for electronic voting.

It is fair to say that Internet voting is not a commonly used means of voting, with only 11 countries having so far used it in any form, and only seven of these 11 countries currently having any intention of using it in the future. However, this low level of usage globally needs to be put into the context of

Internet voting being a relatively new voting technology, and one that has been developing significantly over the previous 10 years. Internet voting seems to fit, for many countries, a niche corner of the electoral system. It is largely targeted at those who cannot attend their polling station in-person on Election Day. In fact many more countries have expressed or shown an interest in the use of Internet voting, especially when they have large numbers of expatriate voters. However, the implementation of Internet voting, according to emerging standards, is a very technical exercise. It can also pose some difficult political questions if the aim is to facilitate the inclusion of large numbers of expatriate citizens in the political process.

The technicalities of implementing Internet voting systems are largely a result of attempts to reconcile the use of Internet voting with emerging and existing standards with which elections and electronic elections are required to comply. These standards include the need for secure online voter authentication, protection of the secrecy of the vote, appropriate transparency mechanisms, testing and certification regimes. The need for secure online voter authentication mechanisms may be one of the biggest hurdles in implementing Internet voting. It presents a challenge for many established democracies, which often do not have an ID card system with secure online authentication mechanisms.

Thematic Issues with Internet Voting

Trust in Internet voting – Trust in the electoral process is essential for successful democracy. Where this trust is lacking the integrity of the overall electoral process may be called into question, undermining the legitimacy of elected institutions and the authority of elected government. The rational choice needed for voters to trust Internet voting seems to require a level of technical expertise that the average voter cannot be expected to have. In order to compensate for the inherent complexity of Internet voting, extra measures need to be taken to ensure that voters have a sound basis on which to give their trust to Internet voting systems. Institutions and experts can play an important role in this process, with voters trusting the procedural role played by independent institutions and experts in ensuring the overall integrity of the system.

A number of mechanisms can be used to enable the development and maintenance of trust in Internet voting systems. One of the fundamental ways in which trust can be enabled is to ensure that information is made available about the Internet voting system. The system must also be trustworthy, and measures to ensure the integrity of the system are important. A vital aspect of integrity is ensured through testing, certification and audit mechanisms. Due to the inherent lack of transparency with Internet voting, it is important to separate the responsibilities for different stages of the Internet voting process. Such a separation of duties means it is more difficult to manipulate the system. Allowing the casting of repeated Internet votes also helps generate trust amongst voters. Making the Internet voting system verifiable, so that the results can be independently verified against the votes cast, is an increasingly important trust mechanism, although this needs to be done in a way that does not violate the secrecy of the ballot. Finally, Internet voting systems should be subjected to various evaluation mechanisms.

The secrecy and freedom of the vote – Ensuring the secrecy of the ballot is a significant concern in every voting situation. In the case of Internet voting in unsupervised environments, this principle may easily become the main challenge. The secret ballot is seen as a tool to protect the freedom of voting so that vote buying and voter coercion do not take place. It is important to note that the use of the secret ballot is not cost-free and may foster a privatization of the electoral process, such that voters may cast a ballot taking into account only their privative interests and not common goals. Secrecy means that voters should be able (some would say required) to cast their ballots alone. Secrecy is thus linked to freedom. Additionally, secrecy also prevents third parties from knowing the vote of a citizen once it has been cast. Secrecy is therefore also linked to anonymity.

Given that an Internet voting system cannot ensure that voters are casting their ballots alone, the validity of Internet voting must be demonstrated on other grounds. One relevant argument is the similarity of Internet voting with postal voting, a method of voting considered to meet standards of secrecy by the Venice Commission. The chance to repeat and cancel an Internet vote is a common argument for the acceptance of Internet voting, as it means that a vote buyer or coercer will not know for sure which ballot will be counted for a voter. Finally, it can be argued (as it has in Estonia) that the principle of secrecy entails an obligation to provide the opportunity for a secret vote, but that voters are free to choose less secret voting options if they desire.

Accessibility of Internet voting – Improving accessibility to the voting process is often cited as a reason for introducing Internet voting. Accessibility for voting systems, closely linked to usability, is an international standard for elections, and is relevant not only for voters with disabilities and linguistic minorities, but also for the average voter. These standards are derived from international conventions, such as the United Nations Convention on the Rights of Persons with Disabilities, which deal with the need for accessibility on a general level. The Council of Europe's recommendations on e-voting include a number of recommendations related to accessibility of voting systems. More technical based standards have also been developed to try and implement these more general standards, such as ISO-29138 and the Web Accessibility Initiative.

Internet voting can have a significant impact on the accessibility of the voting process. It is important that voters, especially those who may have special accessibility issues, are involved in the development of any Internet voting system. The way in which voters are identified, and authenticated, can have a significant impact on the usability of the system, but a balance needs to be found between accessibility and integrity. The voting process itself, and vote verification mechanisms, can also be difficult to design in ways accessible to all. Voters will often demand that Internet voting is available through the end of normal voting, but the duration of voting will need to be determined while considering other factors, such as any requirements for Internet voters to be able to cast a paper ballot. The proliferation of computer operating systems and web browsers presents Internet voting system developers with increasing challenges in making their systems functional on all or most of these operating systems/browsers.

Electoral stakeholder and their roles – The role that stakeholders play in the electoral process is changed significantly by the introduction of Internet voting. Not only do new stakeholders assume prominence in the Internet voting process, such as voting technology suppliers, but existing stakeholders have to adapt their roles in order to fulfill their existing functions. This new network of stakeholder roles and relationships may be difficult to manage well, with some of the demands of stakeholders being contradictory (for example, the different positions that may be taken on the disclosure of information on the Internet voting system).

Central to this new network of stakeholder relationships is public administration, especially the election management body (EMB). Public administration, and the EMB, will establish the legal and regulatory framework for the implementation of Internet voting. This framework will define the roles and rights of the various stakeholders in the Internet voting process. The EMB will also need to manage the implementation of the Internet voting technology, ensure control is maintained over the supplier and facilitate the open involvement of all relevant stakeholders during implementation. An open information policy will be essential to the election management body's interactions with stakeholders to develop trusted relations with these stakeholders while implementing Internet voting.

EMBs need to be sensitive and responsive to opposition and concern about the introduction and use of Internet voting systems. There will likely always be some opposition to such systems, however to ignore opposition and concern is very risky. Even small groups opposing voting technology can have a significant impact by raising concerns which resonate with the public. Election management bodies which fail to respond to concerns about Internet voting may lose control of any public debate in a way that could be fatal for implementation. Proactive engagement with opponents of Internet voting by the EMB and attempts to mitigate these concerns will serve to diffuse potentially damaging public debates on Internet voting. It will also help ensure that Internet voting does not become a, or the, divisive issue in the country's political discourse.

Internet Voting Case Studies

Three cases of Internet voting are reviewed in-depth – Estonia, France and Switzerland-Geneva. Estonia put Internet voting at the heart of their e-government strategy and offered it as a voting option for all voters in elections since 2005. Internet voting is integrated with the use of a smart ID card which all citizens have and which includes cryptographic protocols to allow remote authentication and digital signatures. Usage of Internet voting was low in initial elections, with only 1.9 percent of voters using the Internet to vote in the 2005 local government election. However, usage grew steadily until 24.3 percent of ballots were cast through the Internet in the 2011 parliamentary election.

A second in-depth analysis looks at the French case, where Internet voting has been used since 2003. Internet voting is only used for overseas voters, who elect an Assembly of French Citizens Living Abroad. The Assembly then elects 12 members to the Senate (the upper house of the parliament). Internet voting is one of the voting channels offered to French overseas voters for this election. As of 2012, Internet voting will also be offered to French overseas voters to directly elect 11 members of the parliament.

Switzerland was an early pioneer of Internet voting and first used it in Geneva in 2003, with Zurich and Nauchâtel Cantons soon offering Internet voting. In order to meet its aspirations for direct democracy the Swiss population is regularly consulted on government policy decisions through referenda at all levels of government. In an environment where postal voting was very popular, Internet voting has been viewed as a natural extension of existing voting arrangements. Since 2009, voting for Swiss expatriates is also allowed online for all elections and referenda, and there are plans to increase the use of Internet voting for this group in the future. Non-Internet voting cantons will use Geneva, Zurich and Nauchâtel systems to host expat voters from the non-Internet voting cantons.

Electronic Voting Experiences

The global review of (non-remote) electronic voting experiences found many more examples of electronic voting than Internet voting. The first use of electronic voting machines was in the U.S. in 1975. Although the U.S. had used mechanical voting machines and punch card voting for many decades, it was not until the 1990s that the use of electronic voting machines became more widespread, and countries such as Belgium, Brazil, India and the Netherlands started to implement them in increasing numbers.

In all, 30 countries can be seen to have used electronic voting machines for binding political elections and referenda. Of the 30, 11 countries currently use them and only three (Brazil, India and Venezuela) use them for the entire electorate. Globally, very different trends can be seen between Europe/North America, where the approach is quite skeptical, and South America/Asia, where the technology is increasingly embraced.

Many possible benefits are identified when using electronic voting machines. These include the ability to deal with complex elections, accessibility for voters with disabilities, fewer polling staff, the elimination of invalid ballots, quicker counting, standard adjudication of ballots, accurate tabulation of results and new mechanisms to prevent fraud. However electronic voting brings new challenges, well-illustrated by Ireland, the Netherlands, Paraguay and Germany. In all but the Irish example Internet voting was discontinued despite being used for many years.

The conclusion of the review of global electronic voting experiences outlines a number of trends in the use of electronic voting. The emerging framework of international electoral standards is struggling to catch up with the introduction of technology into the voting and counting process. The use of electronic voting requires a holistic and comprehensive review of the legal and regulatory framework in order to adequately deal with the new mechanisms of administering elections entailed by using electronic voting.

The need for as much transparency as possible when implementing electronic voting is another important theme that emerges from this global review. The use of voter verified paper audit trails is at the heart of debates about how to achieve transparency. Concerns about the security of electronic voting systems is another trend that can be seen over recent years, and in some cases these concerns have led to the discontinuation of electronic voting.

The role that electoral stakeholders need to play in the implementation of electronic voting projects is another trend. Not only do these stakeholders need to broadly support the use of electronic voting, but they need to be included and informed about the decision making process and subsequent developments. As a key stakeholder, the EMB is critical to the success of electronic voting projects. The vital role that it needs to play in the process is also identified. The election management body needs to be capable of implementing electronic voting projects effectively and in a manner which helps build trust in the electoral process. Too many fail to do this and end up delegating key election management functions to technology suppliers.

Finally, it is clear that the field of electronic voting is subject to ongoing technological developments. New functionality is constantly being developed for voting machines, which will continue to raise challenges in the future about the way in which electronic voting is implemented.

Oppsummering av tema 6

Denne rapporten omhandler et av syv temaer som er vurdert på oppdrag av Kommunal – og Regionaldepartementet i forbindelse med forsøk med elektronisk stemmegivning. Hensikten er blant annet å vurdere om innføring av internettstemmegivning vil være egnet for framtidige norske valg. Rapporten fokuserer i stor grad på erfaringer med internettstemmegivning i ulike land og oppsummerer disse landenes erfaringer. Hittil har 11 land gjennomført internettstemmegivning ved bindende politisk valg**.** En kjernegruppe på fire land har benyttet seg av internettstemmegivning over flere valg. Andre land har nylig innført internettstemmegivning, gjennomfører for tiden prøveprosjekter, har testet det ut og ikke fortsatt bruken eller avviklet bruken.

Det er en rekke temaer som springer ut fra forskningen på internettstemmegivning. Internettstemmegivning er i seg selv mindre gjennomsiktig og forståelig enn papirbasert stemmegivning, og skaper derfor betydelige utfordringer for interessentenes tillit til valgprosessen. Valgmyndighetene trenger å implementere en rekke nye tiltak for å etablere og opprettholde tillit til valgprosessen når internettstemmegivning brukes. Det kan være at både institusjoner og eksperter må fylle nye roller i valgprosessen som en tillitskapende mekanisme.

Det å sikre hemmelige og frie valg er en betydelig bekymring ved stemmegivning i ukontrollerte omgivelser, både via internett og på papir. Internettstemmegivning kan gjennomføres med tiltak for å imøtekomme denne bekymringen, for eksempel gjennom muligheten for å kunne stemme elektronisk flere ganger. Dette gir velgerne mulighet til å avgi så mange internettstemmer som de vil, samtidig som det kun er den siste internettstemme som telles. Hvis en velger avgir en stemme under tvang, kan velgeren stemme på nytt og avgi en stemme som er i tråd med ens egen preferanse.

Stemmegivning via internett kan ha betydelig innvirkning på valgets tilgjengelighet. Det er viktig at velgerne, spesielt de som kan ha spesielle tilgjengelighetsbehov, er involvert i utviklingen av ethvert internettvalgsystem. Måten velgerne identifiseres og autentiseres på, kan ha betydelig innvirkning på systemets brukervennlighet, men man må finne en balanse mellom tilgjengelighet og integritet.

Rapporten presenterer tre detaljerte casestudier av bruken av internettstemmegivning - Estland, Frankrike og Sveits-Geneve. Den skisserer hvordan disse er svært ulike eksempler på internettstemmegivning og hvordan man håndterer de mest sentrale utfordringene som internettstemmegivning fører med seg.

Den internasjonale gjennomgangen av erfaringer med elektronisk stemmegivning i kontrollerte omgivelser, viser at det er flere eksempler på elektronisk stemmegivning enn på internettstemmegivning. I alt kan 30 land sies å ha benyttet elektroniske stemmegivningsmaskiner for bindende politiske valg og folkeavstemninger. Av disse 30 er det 11 land hvor maskinene fortsatt er i bruk, og kun tre (Brasil, India og Venezuela) som benytter dem for hele velgermassen. Det er ulike trender internasjonalt, og mens Europa/Nord-Amerika har en ganske skeptisk tilnærming, blir teknologien i økende grad omfavnet i Sør-Amerika/Asia. Konklusjonen etter gjennomgangen av de internasjonale erfaringene med elektronisk stemmegivning skisserer en rekke trender når det gjelder hvordan elektronisk stemmegivning brukes.

2. Introduction

In 2008 the Norwegian Government took a decision, discussed and approved by the Storting (the Norwegian Parliament), to trial the use of Internet voting for Norwegian elections. It was decided that this trial would take place during the local government elections held on September 11-12, 2011. Ten of Norway's 429 municipalities were selected by the Ministry of Local Government and Regional Development (hereafter, "the Ministry") to pilot the use of Internet voting during these elections. Internet voting was available in these municipalities during the advance voting period, from August 10 – September 9.

The primary objectives behind the Internet voting project were to provide better accessibility to voters, to ensure rapid implementation of elections and the efficient use of resources in municipalities, as well as facilitating direct democracy. The Internet voting solution, provided by ErgoGroup and Scytl, was used in pre-trials for youth council elections and local referenda in all of the pilot municipalities from autumn 2010 through spring 2011.

The Ministry, which has responsibility for the oversight of elections throughout Norway, decided to conduct an independent assessment of the Internet voting pilot, and issued a request for proposals for a "Research and Evaluation of the E-vote 2011 Project" covering seven areas of assessment. One of the assessment areas related to the international experience with e-voting. Specifically the Ministry requested:

> *". . . an international overview of information which draws on research from other countries with experience of e-voting in uncontrolled environments. Comparative research into Norwegian and international data about e-voting should also be included. The customer also envisages international research being drawn on to shed light on the other issues (A1-A8)[other areas of assessment] where relevant. The customer is also interested in an overview over trials with electronic voting world-wide."*

The International Foundation for Electoral Systems (IFES) was selected to provide the Ministry with this aspect of research and evaluation of the Norwegian e-voting project. In order to conduct research and evaluation into this topic of assessment, IFES put together a team of experts with considerable experience in electronic and Internet voting:

- Jordi Barrat I Esteve is a constitutional law professor in Catalonia and has been involved in a wide range of electronic voting research projects covering many countries using electronic voting technologies, including Internet voting. He has been directly involved in analyzing both Spanish experiences (e.g., Madrid Participa, EU Constitution Referendum, CETIB) and other international examples of electronic voting (e.g., Venezuela, Mexico, Belgium and France).
- Ben Goldsmith has been involved in managing international elections and providing advice to EMBs for nearly 15 years, including supporting the implementation of a number of election technology projects. He helped the Election Commission of Pakistan to conduct a preliminary feasibility study about the use of electronic voting machines, has written a book on conducting

electronic voting and counting feasibility studies, and presented to conferences on emerging standards for electronic voting.

- John Turner has considerable first-hand experience in conducting multi-channel electronic voting using Internet, SMS text messaging from mobile phones and electronic kiosks in dedicated venues. His experience relates to the design, implementation and evaluation of projects. In addition, he has participated as a member of the Project Board established by the UK Government to select and oversee the evaluation of all types of electronic voting carried out under the pilot programs under legislation introduced in 2000.

Contributions to the analysis presented in this report were provided by Michel Chevallier, Electronic Voting Expert. The team was also supported by Andrea Mandt, a Norwegian Research Assistant, and IFES' Applied Research Center (ARC): ARC Director Rakesh Sharma, Project Manager; Hani Zainulbhai, Research Coordinator; and David Jandura, Research Coordinator. The research also benefited from contacts with election administrators who have been involved in conducting Internet voting and electronic voting projects around the world.

This report represents the results of IFES' research and evaluation on this assessment topic. The report is divided into three main sections on global experiences of Internet voting:

- **Global Internet Voting Experiences** – Provides an overview of global experiences on the use of Internet voting from uncontrolled environments and is based on data sheets which have been developed for nine of the 10[1] Internet voting cases identified (see annexes). The overview looks at the empirical data related to the use of Internet voting from uncontrolled environments, before exploring some of the key thematic issues related to the use of Internet voting. Four thematic issues are identified; the secrecy/freedom of the vote; trust in Internet voting; accessibility; and the role of stakeholders. For each thematic issue, theoretical questions are first discussed before examples of how countries have dealt with the issue are presented. Comparison to the Norwegian Internet voting system is also provided.
- **Detailed Case Studies** – Focus on three examples of Internet voting – Estonia, France and Geneva, Switzerland – which are currently in use, and have been for some years. An overview of the case studies is provided in the main body of the report, with the full case studies included in the annex.
- **Global Electronic Voting Experiences** – Many more countries have experimented with or used electronic voting systems than have used Internet voting systems, so it was not possible to develop data sheets for each one. However, six key examples of electronic voting from around the world were selected and data sheets developed for them: Belgium, Brazil, France, India, Netherlands and USA. These data sheets are annexed to the report and, with a global review of electronic voting experiences, are used to develop themes and trends in the use of electronic voting around the world.

[1] It has not yet been possible to obtain information on the Indian examples of internet voting, that have taken place at a local level in Gujarat.

- One of the problems the assessment team had to grapple with when planning research into both Internet and electronic voting was the criteria to be used in determining whether a country used or did not use Internet or electronic voting systems.
- A pertinent issue with Internet voting systems is that they are regularly used for elections in bodies such as trade unions, political parties, student unions or neighborhood associations. The inclusion of such examples in the assessment would make the number of countries that needed to be reviewed unmanageable. The team felt that there was a fundamental difference in these kinds of elections and elections for institutions of government and public referenda. Therefore, a definition was necessary to clearly identify the context in which a country should be seen as using or having used Internet voting or electronic voting.
- The assessment team agreed that countries would only be considered as having used Internet voting or electronic voting in some capacity if they had used the technology for a "binding vote (elections or referenda) of a political nature."
- Even with this definition some clarification is required, especially for the terms "binding" and "political." Binding is seen as requiring that the vote is legally regulated by public law. The word political is used, in this context with a limited scope, such that elections to bodies such as trade unions or student bodies, which may still be governed by law, would be seen as administrative elections rather than political ones.
- According to this definition a further system of categorization was developed and applied to all countries to determine the status of technology implementation for each country:
- **Never Used** – Countries which have used electronic/Internet voting for elections or referenda which do not meet the definition above are categorized as never having used these technologies. Countries which may be considering the use of electronic/Internet voting, or even developing such systems, but have not actually used them for elections or referenda which meet the definition are also categorized as having never used them.
- **Piloted and Not Continued** – Countries in this category must have piloted electronic or Internet voting for elections or referenda which meet the definition, but then discontinued use of these technologies. A pilot is seen as a use of electronic or Internet voting which is limited in scope to a specific target population for a specific period of time, and for the purpose of experimenting with voting technology. Discontinuing the use of electronic or Internet voting could be indicated by a formal decision to cease piloting the technology or by the fact that the technology is not used in subsequent elections.
- **Ongoing Pilots** – Countries in this category must have piloted electronic or Internet voting for elections or referenda which meet the definition. A pilot is seen as a use of electronic or Internet voting which is limited in scope to a specific target population and for a specific period of time, and for the purpose of experimenting. The ongoing nature of the pilot process is indicated by electronic or Internet voting having been used for the most recent election for that institution and there being an intention to continue piloting for similar elections in the future, or no decision having been made yet as to future pilots.
- **Currently Used in Parts of the Country** – Countries in this category must be using electronic or Internet voting for elections or referenda which meet the definition. The authority to use

electronic or Internet voting must not be limited in duration (although it may be limited to some parts of the electorate) and the technology must actually be in use. This category covers countries where only a few electoral jurisdictions are using electronic or Internet voting and cases where the vast majority of electoral jurisdictions are using the technology.

- **Currently Used Nationwide** – Countries in this category must be using electronic or Internet voting for elections or referenda which meet the definition. The authority to use electronic or Internet voting must not be limited in duration (although it may be limited to some parts of the electorate) and the technology must actually be in use. This category only includes countries where all electoral jurisdictions are using electronic or Internet voting.
- **Discontinued** – Countries in this category must have used electronic or Internet voting for elections or referenda which meet the criteria at some point in the past, but have now decided that this technology is not appropriate and should be discontinued. For inclusion in this category, the use of electronic or Internet voting must have been in a non-pilot situation with the authority to use the technology for an unlimited duration. The decision to discontinue using the previous electronic or Internet voting systems need not be a decision against all electronic or Internet voting systems, but may be a decision to discontinue the use of the technology which was previously utilized.

The final section of this report will focus on electronic voting technologies, and will not cover electronic counting technologies. The Ministry, in its requirements for the project, requested that this topic also cover, “an overview over trials with electronic voting world-wide.” It is fair to say that much of the terminology used in the election technology field is used quite inconsistently, and often terms such as electronic voting and even electronic voting machines (EVMs) are seen to include both electronic voting and electronic counting technologies. Given Norway’s extensive use of ballot counting technologies in many municipalities and counties, it is not believed that the Ministry is interested in an assessment of the use of this technology. Therefore the final section of the report focuses solely on electronic voting experiences using direct-recording electronic voting machines.

The research methodology employed for this chapter is relatively straightforward. There are few examples of binding Internet votes of a political nature, and the expert team had some knowledge of almost all of these examples. In some cases this knowledge was very direct and personal. For countries in which the team of experts had not worked directly on Internet voting, they often had contacts with the EMBs. These contacts were used to access the information needed to conduct the assessment for the Ministry. In many cases these contacts were able to provide reports and information not in the public domain.

3. Internet Voting Experience

As discussed, the definition applied to determine whether countries had ever used Internet voting from uncontrolled environments limited the number of cases of Internet voting which were found to have occurred around the world. This definition ensured that the cases reported here are of comparative value for Norway, and are used in the same kind of binding elections or referenda as used in Norway.

It should also be noted that we do not consider the use of the Internet to send images of ballots via email or to submit them directly through a website to be classified as Internet voting, even if those images are to be electronically interpreted and counted. Sending images of ballots by email would be seen in the same category as postal voting, merely using a different postal mechanism and ballots would normally be printed out and counted by hand. Even when ballot images are counted electronically the process is more similar to that of the electronic counting of paper ballots.

This chapter of the assessment will provide a general overview of the instances of Internet voting from uncontrolled environments before exploring some of the key issues facing the implementation of Internet voting. Four issues are identified and explored;

- Secrecy and freedom of the vote
- Trust in Internet voting
- The accessibility of Internet voting
- The role of stakeholders.

Theoretical questions relating to these thematic issues are first discussed. Examples are then provided to show how countries using Internet voting have addressed these issues. Finally, the Norwegian approach to these issues is discussed.

Overview of Internet Voting

In all, 10 countries were found to have met the definition of using Internet voting from uncontrolled environments at some point, with Norway as the 11th country. These countries are classified in Figure 1 below.

Figure 1 shows that two countries other than Norway, have ongoing Internet voting pilots (the U.S. and India) while one country (the UK) has piloted and decided not to continue the use of Internet voting. Four countries (Australia, Canada, France and Switzerland) use Internet voting for some part of their electorate. One country (Estonia) uses Internet voting on a nationwide level, and two countries (the Netherlands and Spain) have discontinued the use of Internet voting.

While these classifications are useful, they can often cover up significant differences. This is certainly the case with classifying Internet voting systems. For example, Australia, Canada, France and Switzerland are categorized together, but represent very different examples and experiences of Internet voting. In fact each of the 10 cases of Internet voting vary considerably, making it very difficult in some cases to draw comparisons and lessons learned from these examples.[2]

Figure 1 – Countries That Have Used Internet Voting[3]

Country	Classification	Type of Elections in which Internet Voting is Used
Australia	Currently used in some parts of the country	New South Wales (NSW) State elections
Canada	Currently used in some parts of the country	Local government elections
Estonia	Currently used nationwide	Local government elections, Parliamentary elections, Presidential elections, European elections
France	Currently used in parts of the country	Elections to the Assembly of French Citizens Living Abroad
India	Pilots ongoing	Urban Local Body Elections
Netherlands	Discontinued	Water Board Councils and National Parliament (overseas voters only)
Norway	Pilots ongoing	Local government elections
Spain	Discontinued	City of Barcelona referendum
Switzerland	Currently used in parts of the country	Municipal, cantonal and federal referenda
United Kingdom	Piloted and not continued	Local government elections
United States[4]	Pilots ongoing	General elections (overseas voters, predominantly military)

In six of the 11 cases of Internet voting (Canada, Estonia, India, the Netherlands, Norway and the UK) the first use of Internet voting in a country has been at the local government level, often on a trial basis. Estonia and the Netherlands went on to use Internet voting for higher level elections (although the Netherlands subsequently discontinued its use of all forms of electronic voting). Another theme in the use of Internet voting has been the focus, in many cases (Australia, France, the Netherlands, the U.S. and to a lesser extent Estonia), on providing Internet voting for voters who are overseas or away from their home location, and in some cases in providing this service solely for those voters.

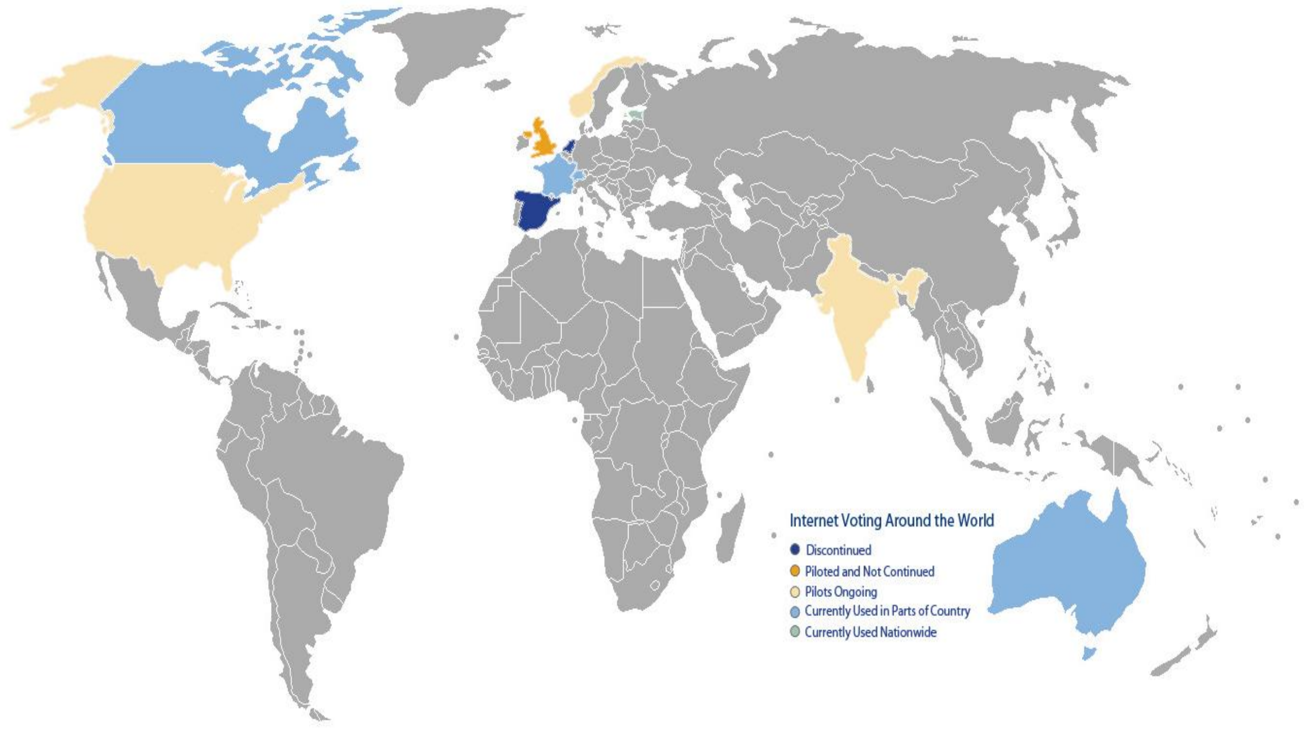
[2] It should be noted that it has not been possible to find out any information on the internet voting system trialed in India beyond vague media reports. These reports do not provide data on the technical aspects of the systems discussed in the comparative analysis below.

[3] Data presented in figures 1 and 2 has been collected from many different sources, including sources such as reports from election management bodies, election management body websites, observer reports, other overviews of internet voting (EAC 2011), the ACE Website and direct contact with election management bodies.

[4] It should be noted that two separate pilots have recently taken place in the U.S., one in Okaloosa County, Florida, in 2008 and one in West Virginia in 2010. The U.S. has a very fragmented electoral management system with decisions on election management being taken at the state or even county level.

Estonia is unique in that it provides Internet voting for all voters wishing to use it for all levels of elections, including the supranational European elections. Other countries do use, or have used, Internet voting for national elections, but they have all restricted the voters who could use this voting option in some way.

Figure 2 – Internet Voting Around the World


Internet Voting Around the World
● Discontinued
● Piloted and Not Continued
○ Pilots Ongoing
● Currently Used in Parts of Country
● Currently Used Nationwide

It is also worth noting that there are generational differences in the Internet voting systems that have been implemented over the course of the decade in which Internet voting has been trialed and used. Earlier Internet voting systems used in the UK and France were conceptually less sophisticated, and failed to implement many of the security, voter authentication and verification mechanisms seen in later Internet voting systems like the Norwegian system. These newer aspects of Internet voting systems have been developed to a large extent to try and meet the emerging framework of electoral standards with respect to electronic voting (of which Internet voting is a subset) and meet existing electoral standards.

In most cases, Internet voting systems have been designed to be used from personal computers in uncontrolled environments (e.g., homes, offices and public spaces). In all but one case, Estonia, no additional hardware is required to vote from such personal computers (Estonia requires an ID card reader). There are some examples of Internet voting which has taken place from controlled environments in polling stations (Finland, some pilots in the UK and U.S.-Okaloosa County) but these examples are not part of this assessment as the Ministry is specifically interested in Internet voting from uncontrolled environments.[5]

A range of motivations have been provided by countries introducing Internet voting. A consistent feature of such reasoning has been the need to enfranchise voting populations which are very mobile and even outside of the country on Election Day. This is especially relevant for expatriate voters and for military personnel stationed overseas during the election. Internet voting is also seen as a way in which people with disabilities can achieve improved access to the ballot, not only in being able to cast a ballot but also being able to cast a ballot without assistance, which maintains secrecy of their vote. In addition, the adoption of technology is seen as a means of demonstrating improved government services and the adoption of digital government. Finally, countries adopting Internet voting have asserted the additional security that Internet voting may provide for ballot boxes, especially when a prolonged period of advance voting is available.

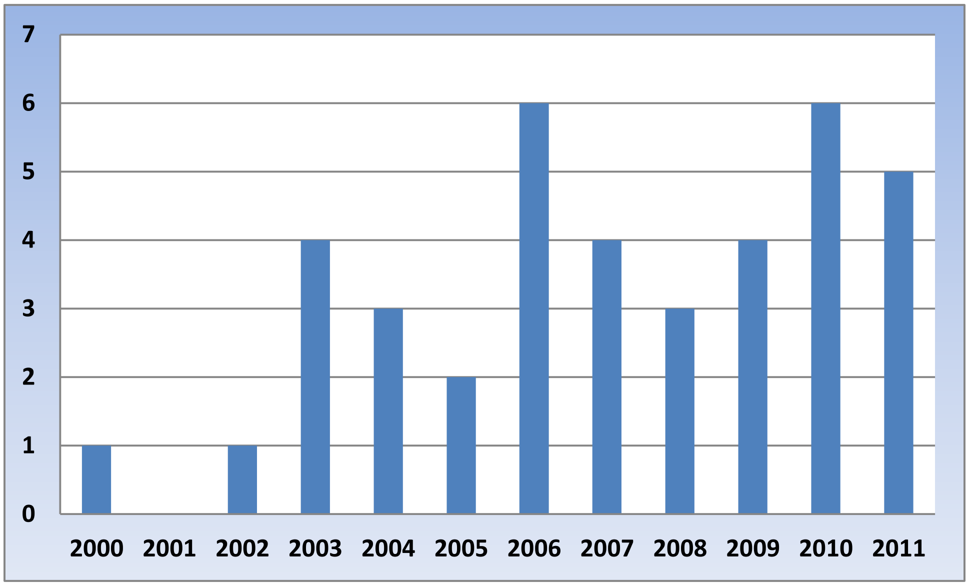
The Growth of Internet Voting

The first use of Internet voting for a binding vote or referendum of a political nature took place in the U.S. in 2000. This example of Internet voting was a trial conducted by the Federal Voting Assistance Program and targeted uniformed and overseas U.S. citizens who have traditionally struggled to participate in U.S. elections. Although the trial encompassed one state and four counties across four other states, it was very small in scale with only 84 voters participating (U.S. Election Assistance Commission 2011: 34).

Figure 3 below depicts the number of countries using Internet voting since then.

[5] A data sheet is provided in the annex for the Finnish example of supervised internet voting.

Figure 3 – Number of Countries Using Internet Voting From Uncontrolled Environments Each Year[6]



After the first trial of Internet voting in the U.S. in 2000, there were no other examples of Internet voting until the UK piloted new ways of voting in local government elections in 2002. The UK continued these trials each year until 2007, with the exception of 2005. Since 2003, Canada, France and Switzerland started to use Internet voting. In 2004 the Netherlands used Internet voting for the first time and in 2005 Estonia held its first election using the Internet. 2006 saw a peak of six countries using the Internet to vote, which was not matched again until 2010.

From 2006, the use of Internet voting has been affected by distrust in some countries towards electronic voting generally, which has had implications for trust in, and acceptance of, Internet voting. This led to a rejection of all forms of electronic voting in Ireland in 2004, the Netherlands in 2007, Paraguay in 2008 and Germany in 2009.[7] In the UK the Electoral Commission recommended, after the 2007 trials, that further trials be discontinued due to concerns about security and testing aspects of the trials, the low levels of public confidence in Internet and telephone voting, and the lack of an overall strategy for trialing new technologies.[8]

Despite these moves away from electronic and Internet voting by some countries, a core group of countries have continued to use Internet voting. This group consists of Canada, Estonia, France and Switzerland. A number of countries have continued to trial and even adopt Internet voting since 2007 with approximately four to six countries using it each year since then. The U.S. held one more small scale trial in 2010; Spain held a referendum solely using the Internet in 2010; Australia held a trial in 2010 and

[6] A primary source of this data was the review of internet voting recently completed by the U.S. Election Assistance Commission (EAC 2011), although other sources were also used, such as reports from election management bodies, observer reports, and direct contacts with election management bodies.

[7] See the section in this report on electronic voting experiences for more details on the reasons for this decision.

[8] See http://news.bbc.co.uk/1/hi/uk_politics/6926625.stm [last accessed on February 29, 2012].

adopted Internet voting in New South Wales in 2011; India trialed Internet voting in 2010 and 2011; in 2011 Norway joined the list of countries using Internet voting with its pilot.

Not all of the more recent experiences of Internet voting have been completely successful. The referendum in the Spanish city of Barcelona encountered problems in relation to voter identification and identity theft, with a prominent voter finding that someone had already logged on with his authentication details and cast a ballot for him. Given this experience it is very unlikely that Spain will experiment with Internet voting again in the near future.[9]

This demonstrates that countries need to be very careful when conducting Internet voting pilots. A poor first experience with new technology can turn electoral stakeholders against the technology in a way that is difficult to repair. This damage to public confidence may bear no relation to the seriousness of the issue encountered or the ease with which it could be fixed.

Eligible Voters and Internet Voting Turnout

Figure 4 shows the numbers of Internet voters compared to the total number of votes cast for each country's most recent elections where Internet voting was an option.

[9] See the data sheet on the Barcelona referendum in the annex for more details on this example.

Figure 4 – Internet Voting Usage

Country and Year of Election/Referendum	Registered Voters	No. Eligible I-Voters	Eligible Categories	No. Internet Voters	Total Votes Cast	Percent Internet Voters
Australia (2011 – NSW State Election)[10]	51,103[11]	431,000 (estimated)[12]	Travelling voters, voters with disabilities, voters in remote locations	44,605[13]	4,290,595	1.04 %
Canada (2010 – Markham Town Elections)[14]	17,231	185,470	All registered voters	10,597	65,927	16.07 %
Estonia (2011 – Parliamentary Elections)[15]	913,346	913,346	All registered voters	140,764	580,264	24.26 %
France (2009 - AFE)[16]	339,382	339,382	All voters (expatriates)	6,026	69,514	8.67 %
India (2011 Gandhinagar Municipal Corporation)	N/A	N/A	All registered voters	N/A	N/A	N/A
Netherlands (2006 – Parliamentary Elections)[17]	N/A	N/A	Overseas voters	19,815	9,854,998	0.20 %
Spain (2010 – City of Barcelona Referendum)[18]	1,414,783	1,414,783	All registered voters	172,161	172,161	100.00 %
Switzerland - Geneva (15 May 2011 – Cantonal and Federal Referenda)[19]	241,780	241,780	All registered voters	21,057	95,540	22.04 %
UK (2007 – Local Council Elections)[20]	N/A	N/A	All voters in pilot elections	17,622	235,222	7.49 %
U.S. – West Virginia (2010 – General Election)[21]	165	N/A	Overseas voters	125	161,548	0.08 %
Norway (2011 – Municipal and County Elections)[22]	168,066	168,066	All voters in pilot municipalities	27,554	104,374	26.40 %

[10] (Barry and Brightwell, 2011).

[11] The number who pre-registered to vote by the internet.

[12] Excluding those outside of the State on Election Day (Allen Consulting Group 2011: 18).

[13] Excludes the 2,259 voters using telephone voting.

[14] (Kitteringham, Brouwer and Tecsa 2010).

[15] http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics [last accessed February 17, 2012].

[16] http://www.assemblee-afe.fr/elections-des-conseillers-a-l-afe.html [last accessed on February 17, 2012].

[17] (OSCE 2006).

[18] http://w3.bcn.cat/fitxers/premsa/informediagonal.071.pdf [last accessed on February 22, 2012].

[19] http://www.ge.ch/evoting/doc/list_of_GVA_ballots.pdf [last accessed February 18, 2012].

[20] Data taken from various electronic voting pilot reports at http://www.electoralcommission.org.uk/elections/modernising_elections/May2007 [last accessed on February 17, 2012].

[21] (Tennant, 2011) and http://apps.sos.wv.gov/elections/results/ [last accessed on February 17, 2012].

[22] http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/elections-results-and-statistics.html?id=654811 [last accessed on February 17, 2012].

It can be seen that the range of voting over the Internet in these most recent cases varies drastically from 125 Internet voters in the 2010 general elections in the West Virginia pilot to over 172,000 Internet voters in the 2010 City of Barcelona referendum. Internet voting usage as a percentage of the overall number of votes cast also varies vastly from 0.08 percent in the West Virginia pilot to 100 percent in the City of Barcelona Referendum.

However, while this data is interesting from a comparative perspective, not all examples are truly comparable. The case of Barcelona's referendum is the exception because in this referendum Internet voting was the only possible means of voting, accounting for the large number of Internet voters and the fact that 100 percent of all votes were cast using the Internet. In all other cases of Internet voting, other channels of voting, normally including paper ballots, were available.

Aside from the Barcelona example, these instances of the Internet being used for elections and referenda can be categorized into two other groups. The first group would be countries which have used the Internet for voting and made this voting channel available to all voters in an election. This would include cases where Internet voting was used for local government elections, but not every local government election, and every voter in such a municipality has the option of using the Internet to vote. Countries falling into the first group are Canada, Estonia, France, the UK and Norway[23]. Of these examples, the percentage of Internet votes cast ranges from 7.49 percent (the UK) to 26.40 percent (Norway). Given that this was Norway's first use of Internet voting this represents a significant demonstration of interest in voting via the Internet. Estonia only managed to achieve its 24.26 percent use of the Internet (the only comparable usage in this group) after four elections using Internet voting, with the first local government elections only seeing a 1.9 percent use of Internet voting.

The second group of countries are those which have offered Internet voting, but not to all voters in an election. Generally such countries have offered Internet voting to voters who are not at their home destination on Election Day, normally because they are abroad and sometimes only to armed forces stationed abroad. In Australia, Internet voting was also offered to voters with disabilities and those who live far away from their polling stations. Countries falling into this category include Australia, the Netherlands, the U.S. and possibly Switzerland.[24]

For this second group of cases, the overall percentage of Internet voters is low because Internet voting is not offered to the whole voting population. The exception in this group is Switzerland. In the case of Geneva Canton, 22.04 percent of votes were cast by the Internet in the May 15, 2011 referenda. While this was the first time that all voters in Geneva could be offered Internet voting, the percentage usage did not differ significantly from previous instances when only 20 percent of voters could be offered Internet voting. This high level of Internet voting must be seen in the context of trust and acceptance that has built up amongst voters over the eight years Geneva has been providing the opportunity to vote through the Internet.

[23] And sometimes Switzerland – Geneva, see footnote 23.

[24] Referenda are generally held at the same time for multiple levels in Switzerland. When a federal referendum is being held, internet voting can be offered to no more than 20 percent of registered voters. Only in May 2011 and November 2011 have referenda been held which did not include a federal referendum, therefore allowing all citizens in Cantons using internet voting to be offered the opportunity to use the internet to vote.

Other examples in this group exhibit much lower levels of overall Internet usage, from as little as 0.08 percent in West Virginia to 9.4 percent in France. Given that only parts of the electorate were offered Internet voting as an option in Geneva's elections, it may be more appropriate to assess the percentage usage of the Internet against the number of votes cast by voters who could have voted using the Internet. As an example, in the 2006 Netherlands Parliamentary Election there were 28,170 overseas votes cast, meaning that the 19,815 Internet votes cast represents 70.34 percent of all votes cast by overseas voters.

Alternative Voting Channels

The City of Barcelona referendum was the only case where the use of the Internet for voting was compulsory, with no other voting channels being made available. In all other cases the casting of a paper ballot, either in a polling station or by mail, was possible. In some case alternative channels, such as telephone voting (in Australia and the UK), were also provided which gave the voter a wide choice of channels to participate in the election.

The Norwegian use of Internet voting follows the general trend in not making the use of the Internet compulsory and allowing paper balloting as an alternative to Internet voting. In fact this paper balloting option is provided through a number of mechanisms in Norwegian elections. Early voting is possible from approximately two months before the election; advance voting (in more locations) is available for approximately one month before the election; and postal voting is also available for voters living abroad.

The use of multiple channels does present an additional administrative challenge in that mechanisms need to be in place to ensure that results from all of the channels available are included in the count and results. In fact this problem was experienced at the recent Norwegian Internet voting trial in one county with Internet votes from Hammerfest Municipality not initially being included in Finnmark's county election results.

Period of Internet Voting

In general, Internet voting is offered to voters in advance of Election Day and for a period of between one and two weeks. The City of Barcelona referendum is the slight exception to this in that it only allowed Internet voting and did so over a five-day period.

The Norwegian system of Internet voting follows the more standard approach of allowing Internet voting only in the advance period of voting, although it provides this opportunity for a much longer period than most other instances of Internet voting – for one month. However, this is in line with the period provided for advance paper balloting in Norway.

Voter Identification and Authentication Mechanisms

The authentication of voters when using Internet voting systems is a critical issue for the integrity of the election. It is essential that mechanisms are in place to ensure that only registered voters are able to log on and cast their vote. Varied approaches have been taken to this issue across the 10 cases of Internet voting.

In four cases, pre-registration was required for Internet voters (Australia, Canada-Markham, France, the Netherlands, and the U.S. – West Virginia). In the course of this pre-registration additional voter authentication codes are created and provided to the voter. These codes are then used, sometimes with other voter authentication data, in order to identify and authenticate the voter before they cast a ballot online. In three cases[25] no pre-registration was required for voters wishing to cast their ballot by the Internet (Estonia, Spain-Barcelona and Switzerland-Geneva), with Norway also taking this approach.

Each of the other cases adopted differing voter identification and authentication mechanisms. In fact Spain-Barcelona used three different authentication mechanisms for voters:

- Digital official certificates already accepted in other e-procedures with the Barcelona City Council (e.g. the one issued by CatCert, the official Catalan Authority for Digital Certificates)
- A one-time password sent to a cellular phone (the citizens received this password after registering on-line and providing their ID number, birth date and phone number)
- Partners' websites (e.g. Universities, banks) with their own authentication logins (the e-voting system was embedded in partner websites so citizens did not need new logins and passwords)

Geneva, Switzerland used a combination of authentication codes issued specifically for the election and data which is personal to the voter. For each voting operation, the voters receive (by post) a single-use voting card containing a unique number enabling them to be identified in the voting management system, irrespective of the voting channel (electronic, postal, polling station) they choose. For online voting, the voter number and password are completed by voter in the system in addition to two shared secrets not presented on the voting card: their birth date and their municipality of origin.

The Estonian Internet voting system relies heavily on the country’s national ID card, which all citizens are required to possess from the age of 15. Citizens are issued two passcodes to be used with this chipped picture ID card. This allows citizens to use the ID card to digitally sign documents. Under Estonian law, such digitally signed documents using the ID card are legally equivalent to manually signed documents. The ID card is widely used for online access to many government websites as well as for commercial institutions such as banks. Authentication using the ID card requires a card reader, but these are inexpensive, easy to buy, and widely available on computers in public spaces (such as public libraries and Internet cafes).

More recently it has also been possible to authenticate voters in Estonia through a mobile-ID system where a mobile phone can be used to act as an ID card and a card reader at the same time. The same functionality in terms of authentication and digital signatures is possible through this mobile-ID system (Madise and Vinkel (no date): 3).

In this regard, the Norwegian Internet voting system shares the most similarities with the Estonian system as it uses existing identification mechanisms which are used for other services. Three of these identification mechanisms were used for the 2011 Internet voting pilot, the main one being the MinID, a

[25] In the final case, the UK, different voter identification mechanisms were used for the different pilots in 2007, with some requiring pre-registration and others not.

personalized log-in system for accessing online public services in Norway. The MinID authentication process requires the user to enter a password to conduct the first phase of voter identification and authentication; a second code is then sent to the voter on their registered mobile phone. The second code is used to complete the authentication process online before the voter can proceed to cast a vote. It is a one-time code, so that if the voter wishes to cast a repeat vote, the entire authentication process is repeated and a new code is sent to the voter to allow them to complete the login process.

Legal Basis for Internet Voting and Challenges

The legal basis for Internet voting varies from country to country, as does the general electoral legal framework. In three cases (Estonia, France and Switzerland-Geneva) the appropriate election laws have been amended to allow the use of Internet voting on an ongoing basis – which is to be expected as these countries have been using Internet voting for an extended period of time. In two cases (Netherlands and Spain-Barcelona) electoral legislation has been changed specifically to allow the use of alternative voting channels on an experimental basis or regulations have been passed for the specific elections/referenda for which Internet voting has been used. In three cases (Australia-NSW, Canada-Markham and the UK) there is ongoing authority under electoral legislation to experiment with alternative voting channels, including Internet voting. In all cases there has been a clear legal basis for conducting Internet voting.

Despite the clear legal basis, Internet voting has not gone unchallenged in these countries. Internet voting has been very controversial in some countries, and in such an environment it is to be expected that complaints will be raised with EMBs. In five cases (Australia-NSW, Canada-Markham, France, the Netherlands and the UK) complaints against the legality of Internet voting or the legitimacy of results produced by Internet voting have never progressed into a court challenge. In Switzerland-Geneva a legal challenge was made, but little evidence was provided that Internet voting had not led to accurate results and the legal challenge was not upheld. In Spain-Barcelona an ongoing legal case related to voter personation is still ongoing at the time this report was submitted.

In the remaining case (Estonia) the legal challenge to Internet voting has been more serious. In Estonia, two legal challenges were made against Internet voting. The first challenge came from Arnold Rüütel, then-President of Estonia in 2006, who challenged the use of Internet voting on the basis that it violated the principle of one person, one vote. President Rüütel was of the view that the possibility to change one's Internet vote during the period of advance polling gave voters an advantage over those that attended traditional polling stations and thus violated the constitutional provision of uniformity in elections. The Supreme Court of Estonia subsequently reviewed the legislation, held that it was constitutional, and denied the challenge, ordering President Rüütel to promulgate the challenged law (Estonian Supreme Court 2005).

The second legal challenge to Internet voting in Estonia came in March 2011 after the Parliamentary Election. The petition before the Supreme Court sought to invalidate the electronic results during the election on the basis that it was possible for a virus to block the submission of an Internet vote without the voter knowing this had happened. The petitioner demonstrated that this could happen with the assistance of several other voters (who consented to the demonstration). However, as all of the participating voters consented to having their votes blocked by the virus, the Court found that no violation of their rights took place. In the absence of proof that other voters suffered from this virus and therefore had their rights violated, the Court found no evidence that the reported result was in any way inaccurate and therefore it rejected the legal challenge (Simmons 2011, Rikken 2011).

Trust in Internet Voting

Trust in the electoral process is essential for a successful democracy.[26] When trust is lacking, the integrity of the overall electoral process may be called into question, which undermines the legitimacy of elected institutions and the authority of the elected government. These are serious consequences and EMBs need to ensure that they take all measures to establish and maintain trust in the electoral system. However, the notion of trust is difficult to conceptualize. Trust itself can be fickle, resting on people's perceptions of facts rather than the facts themselves.

This section of the report will begin by discussing some general theoretical aspects of trust, trust related to systems, and why trust is an issue for Internet voting. Next the report will discuss a range of mechanisms that can be employed to enable trust in Internet voting systems. This framework of mechanisms is largely based on a paper by Spycher, Volkamer and Koenig presented at the Norwegian E-Vote Conference prior to the 2011 local government elections (Spycher, Volkamer and Koenig 2011). The IFES team identified a number of other mechanisms which are also included in the report, as well as elaborating on some of the mechanisms previously identified. For each trust mechanism, the report explains the mechanism and details international practice[27] and the way in which such mechanisms have been implemented in the Norwegian Internet voting system.

Key Aspects of Trust

Electoral systems face two challenges in delivering credible elections; they need to deliver an election that reflects the will of the voters while also convincing key electoral stakeholders that they have delivered an election which reflects the will of the voters.[28] While other systems' integrity may be self-evident from the results that they produce, electoral systems rely much more on procedural safeguards than self-evident proofs of integrity. Therefore, there must be trust in the process itself for the results to be trusted. Without such trust even legitimate results may be rejected.

Understanding Trust

There are many definitions for trust, often based on the academic approach that is being used to analyze trust. From a general sociological perspective Simmel defined trust as, "a blending between knowledge and ignorance" (Pieters and Becker (2005): 3). Coming from the perspective of trust in on-line systems Corritore et al define it as, "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited." (Corritore, Kracher and Wiedenbeck 2003: 740)

These definitions help to uncover some aspects of trust which will be important when considering the role of trust in Internet voting. Clearly there is no need for trust where full knowledge exists, but trust

[26] See the ACE Project website discussion of guiding principles for maintaining confidence in the electoral process - http://aceproject.org/main/english/et/et20.htm [last accessed on March 5, 2012].

[27] It should be noted that some of the examples of international experiences relate to internet voting in controlled environments, but only when the challenges are comparable between controlled and uncontrolled environments.

[28] Avergou et al refer to this as trust v trustworthiness (Avgerou et al 2007: 3)

also cannot exist in the absence of any knowledge. Trust represents a rational decision on the part of the trustor to trust the trustee, and this decision is not possible in the absence of knowledge. Decisions in the absence of knowledge are more aptly considered as faith-based. While average voters have little knowledge of traditional paper based systems, they likely know enough to understand the basic mechanics of the voting and counting processes. This is not the case with Internet voting, which requires much more technical or procedural knowledge to have a sound factual basis for trusting the system.

Trust also involves an element of risk. Trust has no meaning if there is no risk involved in putting trust in an individual or system (Corritore, Kracher and Wiedenbeck 2003: 741). Therefore there is a possibility that the trustor will not achieve their anticipated outcomes when placing trust in the trustee, and trust entails, "an unavoidable element of risk and potential doubt" (Lewis and Weigert 1985: 968). However, there will be a "confident expectation" by the trustor that these outcomes are likely to be achieved (Corritore, Kracher and Wiedenbeck 2003: 742).[29] Finally, trust entails vulnerabilities and the possibility of an exploitation of the relationship between the trustor and trustee, but the trustor must believe that this exposure will not be exploited in a manner detrimental to their interests (Corritore, Kracher and Wiedenbeck 2003: 742).

These elements of trust are all evident in Internet voting systems. Those putting trust in Internet voting systems will confidently expect that the vote they cast will be recorded and included in the results and that only legitimate ballots are counted. There is of course a risk that this will not be the case, and certainly a natural perception (given the inherent complexity and lack of transparency with Internet voting systems) that the risk is greater with Internet voting systems than with paper balloting. Internet voters also have to believe that the information they provide will not be exploited, for instance by linking their identity to the value of the vote that they cast.

Academic research has identified one of the principle roles of trust as providing, "the means to decrease complexity in a complex world by reducing the number of options one has to consider in a given situation" (Corritore, Kracher and Wiedenbeck 2003: 738). By placing trust in individuals and systems, the decision making process is reduced to manageable proportions (Lewis and Weigert 1985, 968-9) and the possibilities for action are created (Pieters and Becker (2005): 4). A reduction in complexity is especially relevant for technology systems like Internet voting.

Lewis and Weigert argue that;

> *"An adequate conceptual analysis of trust begins by recognizing its multi-faceted character. It has distinct cognitive, emotional, and behavioural dimensions which are merged into a unitary social experience" (Lewis and Weigert 1985: 969)*

Having considered how trust can be conceptualized, we will now examine how trust is established and maintained. Obviously trust will be enabled in different ways in different situations. Research into human-computer interactions in online situations (highly relevant for Internet voting) indicates a

[29] A decision where there is not a reasonable expectation of achieving the intended outcome is better characterized as a gamble.

number of common cues which help to convey trustworthiness in online environments. These include the ease of navigation, good use of visual design elements, professional images of products, the absence of typo errors, a professional look for the site, ease of searching and ease of transactions (Corritore, Kracher and Wiedenbeck 2003: 746-7). While the cues identified by this research are intuitively understandable, it is interesting to note how cosmetic some of them are, and relatively unrelated to the trustworthiness of the system.

The proper functioning of online systems is also vital for establishing and maintaining trust. In fact Lee and Mornay argue that, “Empirical studies of trust in automated machines show that performance and trust increase following a similar learning curve as long as there are no errors” (Corritore, Kracher and Wiedenbeck 2003: 745-6). Therefore, trust and performance are positively related with online systems. The problem for Internet voting systems is that it is not easy for the average voter to assess the accurate performance of the system.

It is also important to note that Lee and Mornay “. . . found that errors lead to a precipitous drop in trust roughly proportional to the magnitude of the error. If the error is not repeated, performance recovers immediately, but recovery of trust to prior levels occurs over a longer time” (Corritore, Kracher and Wiedenbeck 2003: 745-6). This point is strengthened by Pieters and Becker, writing specifically about Internet voting systems, who argue that trust is fragile and small mistakes in a system can actually have devastating consequences for trust in the system (Pieters and Becker 2005: 4).

Pieters and Becker identify an important aspect of system trustworthiness, compared to individual trustworthiness; they assert that it is far more difficult to make a serious estimation of the reliability of the system (especially very complex systems such as Internet voting systems). Technical experts on the system may present arguments as to why the system should be trusted, but only similarly qualified experts will be able to fully understand these arguments. Proxy trust, which relies on expert third parties, plays a significant role in trusting Internet voting systems. The consequence of this reliance on third parties is that the attitude involved in trusting such complex systems ‘comes much closer to “belief” in the authority of people’ (e.g. experts). This belief in the authority of experts need not be entirely based on the people/institutions that provide this oversight; it can also be based on the procedural system of oversight too. Such a system might foresee roles for multiple, independent experts. However, Pieters and Becker argue that this sort of trust, “can unexpectedly and quickly turn towards its opposite. In this way a high level of trust can change into severe disappointment and grave distrust” (Pieters and Becker (2005): 4).

A final issue related to our understanding of trust needs to be made. There is a significant difference between trust and a passive attitude. While they may lead to similar kinds of actions, trust is a much more stable attitude, whereas passivity is problematic. Passivity is an absence of opinion and represents a situation which can quickly change, possibly in a negative direction relating to trust in the system. When passivity turns to distrust it may be too late to rebuild trust in the system (Pieters and Becker (2005: 5).

This understanding of the nature of trust and the ways in which it can be established and eroded will be important as we move on to look more specifically at the mechanisms that can be employed with Internet voting systems (and in fact many systems) to ensure that voters and other key stakeholders are willing to trust the results generated by Internet voting systems.

Trust and Internet Voting

Paper-based voting is relatively simple to understand and it is easy to observe all of the steps of the process in order to verify that the overall system functions correctly.[30] Given that Internet voting is based on computerized processes, the average voter will likely struggle to understand the technicalities of Internet voting systems and will not be able to provide any meaningful oversight of the Internet voting process. An average citizen is able to observe some external evidence of the functioning of Internet voting systems, but this evidence will likely be of little value because they do not demonstrate the correct performance of the system itself. Even if more detailed technical documentation is made available, the vast majority of voters will not understand this information.

Chantal Enguehard uses the term “dematerialization of the ballot” to emphasize that electronic voting eliminates physical ballots, that is to say, evidence that can be understood by the average citizen. Electronic ballots can also be seen as dematerialized components as they are only based on a digital layout and therefore they will remain a barrier for a common voter (Enguehard 2009).

Given this gap in understanding for the average voter, the rational decision to trust Internet voting systems is much more difficult to make and likely to be more unstable unless additional measures are taken to enable trust by stakeholders.

It should also be noted that trust in Internet voting needs to be viewed in the context of general trust in government institutions. In the Norwegian context, Christensen and Laegreid note that there is a strong relationship between trust in different government institutions such that, “People with a high level of trust in one institution also tend to trust the other institutions, while distrust in one is related to distrust in others” (Christensen and Laegreid 2003: 23). The OECD’s Better Life Index finds higher than average (for OECD countries) levels of voter turnout and trust in political institutions in Norway, which they use to argue that Norway enjoys high levels of trust in government and public administration.[31] This high general level of trust in public administration will have an influence on the level of trust in Internet voting in Norway.

Establishing and Maintaining Trust

The mechanisms for establishing and maintaining trust in Internet voting systems outlined below are largely based on a paper written by Spycher, Volkamer and Koenig on mechanisms for establishing trust in the Norwegian Internet voting system. Several additional mechanisms have been added to those identified in the paper. The theoretical foundation of each mechanism for establishing trust is detailed where relevant. International examples and experiences of implementing trust mechanisms are also

[30] Postal voting would be an exception to this, and paper based remote voting suffers from many of the same challenges as unsupervised internet voting.

[31] See http://oecdbetterlifeindex.org/countries/norway/ [last accessed on February 1, 2012].

outlined, as well as the way in which the Norwegian Internet voting system implements such mechanisms.

Transparency

Transparency is an essential mechanism for building and maintaining trust in Internet voting systems. As mentioned, trust in Internet voting represents a rational decision on the part of the trustor about the merits of Internet voting. A rational choice on whether or not to trust cannot be made in the absence of information about the system. Therefore systems have to be transparent so voters and other stakeholders can gather information and make a rational decision to trust. The need for transparency is not unique to Internet voting. Paper balloting also needs to be transparent if it is to be trusted; and, as discussed above, Internet voting is inherently more difficult to observe and understand than paper balloting. Countries implementing Internet voting have to place trust in proxies who can and do analyze the Internet voting system. Their analysis of the system will require a high level of transparency of system documentation and information; otherwise proxies will not be able to declare any well-founded opinions on the reliability of the system. Common documents which need to be made available in order to allow expert proxies to conduct meaningful analysis of the functioning of the Internet voting system include: source code for the system, test plans and results, audit reports, system specifications and user manuals, and any other information necessary for a full assessment of the system.

There are two aspects to the transparency of information related to the Internet voting system: access to the information itself, and the ability to disclose the findings of analysis conducted on the basis of this access. Both are important for the overall transparency of the system, and in order to enable trust in the system.

Access to information can be a touchy issue from a number of aspects. System administrators may be unwilling to disclose all aspects of a system as doing so may make it easier for people to manipulate and defraud the system. A common demand by stakeholders is that the voting system source code is made available for public scrutiny. The purpose of this disclosure is to allow stakeholders to review the code and identify any instances where the system does not function correctly, either because of a mistake or a deliberate attempt to manipulate the system. Suppliers are often reluctant to provide this access as they consider the code to be proprietary in nature and the result of significant investment on their part. Similarly, certifying/reviewing organizations may be unwilling to disclose all aspects of their work as this may provide information on the methodology that they use, which could be useful to competitors.

In fact, significant debate has taken place around the merits of disclosing source code. The issue of system security is obviously very important but the general tide of opinion seems be moving towards making electronic voting, and Internet voting, source code accessible.[32] While the publication of source code is an obvious transparency mechanism and one which may represent an important cue conveying trustworthiness, its actual impact may be less significant for a number of reasons. Only a small percentage of IT-literate stakeholders will be able to review the source code in any meaningful manner.

[32] A good example of this can be seen with Scytl, the supplier of the Norwegian internet voting solution and one of the leading suppliers of internet voting solutions. Scytl did make its source code available, something it had not done on previous internet voting projects.

Furthermore, as code for systems such as Internet voting will be complex and long, a full review of the source code will represent a significant investment in time and effort. This may be an investment that few, if any, are willing to make on a voluntary basis. Stakeholders such as political parties and observers may be willing to employ IT experts to conduct a review of the source code, but it is also possible that, even when source code is published, no one will conduct a meaningful review of it. Nevertheless, the mere fact that source code is published may serve as a deterrent against the deliberate manipulation of the Internet voting system. However, the publication of source code will not help to identify genuine mistakes if it does not lead to competent stakeholders reviewing the code.

One of the ways that Internet voting suppliers can try to mitigate the commercial risk of providing access to their source code is through limiting access to those willing to sign a non-disclosure agreement (NDA). NDAs limit the information that those reviewing the code can disclose. While such agreements may help to meet the conflicting demands of transparency and commercial interests, they are not without their problems especially where they overly limit the possibility for reviewers of the code to publish the results of their review.

There are many ways in which transparency can be improved for trusting Internet voting systems. Not surprisingly, different countries implementing Internet voting have taken differing approaches to the challenge of transparency. While all of the countries using Internet voting allow election observers, observing Internet voting is incredibly difficult as it lacks the focus provided by a polling station and count center environment. Attempts, therefore, have been made to achieve a more general level of transparency in other ways. In two cases of remote Internet voting (Estonia and Spain-Barcelona) access was provided to the source code for those signing a NDA. This NDA agreement was in issue in the Finnish supervised Internet voting pilot, where Electronic Frontier (EFFI) refused to sign this NDA because it foresaw too many limitations on their disclosure and subsequent handling of data (Vähä-Sipilä 2009; Tarvainen 2008). No system seems to have been fully open source to date (Norway will be discussed below). The Dutch system was the closest to open source although access to the source code was only provided after the election, which undermines the transparency and benefits to some extent.

Other more general transparency mechanisms include the provision of access to system documentation, which is done in two cases (Estonia and the Netherlands) and official observation of the opening and closing of electronic ballot boxes for Internet voting, which is done in one case (Australia-NSW). In Estonia, however, the Election Assessment Mission (EAM) deployed by the Organization for Security and Co-operation in Europe’s Office for Democratic Institutions and Human Rights (OSCE/ODIHR) in 2011 recalls that “testing is a crucial exercise to find any deficiencies in the system. The NEC made a substantial effort to test various components of the Internet voting, including by members of the public. However, reporting on the performed tests was often informal or kept secret” (OSCE/ODIHR, 2011: 10). The EAM also commented on the NDA that was required by the supplier of the Internet voting system, stating that: “observers were allowed to view the source code of the voter application only after signing a non-disclosure agreement, which limited the observers’ ability to comment on the source code and, therefore, transparency of the system” (OSCE/ODIHR, 2011: 14). If those providing oversight functions cannot express their opinions, it is to be wondered what purpose is served by providing this access.

The Norwegian Internet voting system was meant to be open source, and source code was published online in advance of the election.[33] However, late changes were made to the source code and the final version of the code was not published online until after the election.[34] The Ministry did contract an external expert to do an independent review of the code as well as system testing (Vollan 2011: 4), a process which did find errors which were subsequently corrected. Norway made significant attempts to educate and inform electoral stakeholders about the functioning of the Internet voting system through online documentation, briefings to electoral observers and a live-streamed decryption and counting ceremony for Internet votes. In many ways the Norwegian Internet voting example has made the most consistent efforts to implement a transparent Internet voting system, although even here improvements could be made.

Integrity of the System

The trustworthiness of a system is not the same as a system being trusted. The trustworthiness of a system is, however, an important determinant of trust whether the system is reliable and delivers the intended results. If this is the case, then a system is more likely to be trusted. As Corritore *et al* stated, "competence is one of the cognitive cues for trust" (Corritore, Kracher and Wiedenbeck 2003: 741). Obviously, enabling trust is not the primary reason for designing and implementing systems which are reliable; systems are inherently designed to deliver their intended objectives. There are a range of features that can be indicative of a reliable Internet voting system reliability; these include, but are not limited to;

- Voter authentication mechanisms – These mechanisms aim to ensure that only legitimate voters can cast a vote, and it is the registered voter who is actually casting the Internet vote
- Equality of the vote – The overall electoral system needs to ensure that Internet voting does not allow the possibility for voters to cast and have counted multiple votes
- System security mechanisms – Such mechanisms protect the secrecy and integrity of the online voting transaction, ensure online transactions cannot by monitored/manipulated and protect online servers holding voter and vote data
- Cryptographic protocols – As data is passed between the Internet voting client (the voter's PC) and the vote server this data can and should be encrypted to ensure the voting data cannot be intercepted and the secrecy of the vote violated, (likewise, the data held in the vote server should be encrypted to ensure that the data cannot be accessed without the necessary decryption key)
- Encryption key control – The process of generation and possession of the encryption key needed to decrypt voting data is an important part of the Internet voting process, and an important mechanism to protect against unauthorized access to the data

[33] Access to the source code was based on a general license published on the web that allows review of the system for non-profit purposes.

[34] It was published on 7 October, and can be found at www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/source-code/click-here-for-access-to-the-source-code.html?id=646007 [last accessed on February 29, 2012]. The Ministry did indicate that even though the final version of the source code was not published online until after the election, it was available to anyone wanting access before this publication (email of February 9, 2012).

In terms of international practice, voter identification and authentication mechanisms were covered in the general overview of global Internet voting experiences. All of the Internet voting systems include mechanisms to ensure that only one vote, Internet or otherwise, is counted for each voter. The Norwegian system requires that all paper votes are processed before Internet votes are counted,[35] so that any Internet voter also casting a paper ballot only has their paper ballot counted.

All of the Internet voting systems, including the Norwegian one, encrypt data transmitted from the Internet voting client to the server. It is not clear whether all or some of the systems maintain the encryption of the voting data on the server once received, but the Norwegian Internet voting does maintain this encryption until the counting process. In the Norwegian case the key required to decrypt the Internet ballots is generated at the start of the Internet voting process and divided between 10 identified keyholders. These keyholders represent the main Norwegian political parties and are required to attend the decryption and counting ceremony for the Internet votes. Only six parts of the decryption key are required to decrypt the votes, meaning that a majority of the keyholders would have to collude to break the Internet vote encryption (as well as the Ministry, which is in possession of the vote server) and that the decryption is still possible if some of the keys are lost.

Testing/Certification/Audit

Testing, certification and audit procedures are important in the development of any complex system. While these procedures could be considered under the heading of integrity, they are important enough to be dealt with separately. The Council of Europe defines these different procedures in the following way (Council of Europe 2011a: 10-11);

- Test - The process of verifying that the subject works as expected
- Certification - A process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it at least includes provisions to ascertain the correct functioning of the system. This can be done through measures ranging from testing and auditing through to formal certification. The end result is a report and/or a certificate
- Formal certification - A type of certification that is official and conducted only before the Election Day and leads to the issuance of a certificate”
- Audit - An independent pre- and/or post-election evaluation of a person, organization, system, process, entity, project or product which includes quantitative and qualitative analysis

Given that verifiable systems may be problematic (discussed later) and trust by proxy is necessary, the establishment of formal certification procedures might be seen as a suitable way to check key elements of the Internet voting system that an average citizen cannot understand. If the certifier issues a positive report, both electoral authorities and the citizenry would have a well-founded basis on which to trust the accurate performance of the Internet voting system.

However, certification covers a wide range of possible processes. Taking into account the guidelines approved by the Council of Europe on e-voting certification procedures, it is easy to see that the generic

[35] Although the preliminary tally of internet votes began when paper ballots were still being processed.

title of certification is afterwards translated into different nuanced meanings so that certification would encompass both a formal procedure and other control mechanisms such as tests and audits.

Internet voting countries do not tend to adopt a formal certification process because some technical components (e.g., client's PC, on-line software) are difficult to submit to such an intensively structured procedure where a certifier has to verify, before the elections, how all the components comply with a set of requirements previously established. The alternative consists in implementing a set of tests and audits that, although being less standardized, intend to provide sufficient evidence of system integrity.

Nearly all cases of Internet voting implement some form of audit to ensure the system operated correctly and according to the specifications developed for the various systems. Only one of the countries does not seem to have implemented any audit mechanisms, the UK. The UK was a trial of Internet voting and therefore it is understandable that audit mechanisms may not have been implemented for this trial, although implementing some sort of audit is an emerging standard for electronic voting systems (Council of Europe 2004).

Six Internet voting cases conduct some level of independent system auditing (Australia-NSW, Canada-Markham, Estonia, France, Spain-Barcelona and Switzerland-Geneva), with these audit reports sometimes being publically available on completion. Additional audit mechanisms which have been used include the existence of an auditor module for the Internet voting system, which logs and reports all transactions on the database (Canada-Markham), the conduct of mock/test elections (Australia-NSW, Canada-Markham, Estonia and Switzerland-Geneva) and statistical analysis of the results to identify any irregularities which might be caused by manipulation of the results (Switzerland-Geneva). In the Netherlands, the existence of end-to-end verifiability seems to have been seen as a sufficient check that the system worked correctly.

Estonia conducts several tests and audits, but not a formal certification (OSCE/ODIHR: 13-14). That is to say, there is no independent entity before the election issuing a formal document attesting that the technical components comply with a given set of standards. The Estonian election authorities hire an audit firm that assesses whether the Internet voting system is performing the tasks it is meant to and issues a report after the election. There also are other technical tests that cannot be classified as a formal certification. In other countries, the framework is more or less the same. While not accepting a formal certification, different tests and audits intend to achieve the same goal.

The mandate provided to any organization testing, certifying or auditing any Internet voting system is also important. In Estonia, for instance, electoral authorities emphasize that an international audit firm is always hired to conduct a supervision of the process, but actually its scope is limited to verifying whether the Internet voting system is following the operational manual (OSCE/ODIHR: 16). Auditors would not be able to wonder whether this document is sufficient for the needs of Internet voting because their role is only to check its implementation, not to discuss its content.

Norway does not include a formal certification, but its approach is slightly different. It argues that in this case Internet voting procedures can be submitted to an end-to-end (E2E) verification. Both supervisions in conjunction with the disclosure of all relevant data concerning Internet voting devices may provide the same or even higher degree of confidence than formal certification. This leads to the debate outlined in the previous paragraphs becoming somehow meaningless. However, it is worth noting that E2E mechanisms still rely upon tasks that can only be conducted by IT experts. Therefore, this solution may ease the controls over the voting application and namely allow any interested expert to carry out his/her own verification, but, in contrast to what happens with traditional paper-based elections, average citizens will still remain excluded.

The Internet voting system implemented in Norway did include an auditor module for monitoring transactions on the system. It also employed several organizations to provide system and security audits. In addition the Ministry contracted an independent auditor to check that key stages of the vote authentication and counting processes were conducted accurately and recorded votes were not changed during the cleansing, mixing and tallying stages of the process.

Separation of Duties

Pieters and Becker argue that the involvement of multiple stakeholders at all levels of elections and all stages of the process ensure that the opportunities for tampering with an election are more difficult and more likely to be discovered. Such compartmentalization of roles prevents any one party from exercising too much responsibility and power over the system (Pieters and Becker (2005): 11). Spycher et al point to the benefit of distributing secrecy critical duties so it is not possible for one single entity to break the secrecy of the vote. It is also a measure that is easy to explain, making it suitable for enabling trust. The possibility for such separation of duties to enable trust does depend on the selection of responsible parties to conduct those duties (Spycher, Volkamer and Koenig 2011: 6). Therefore the entities amongst which duties are divided will need to be carefully selected. It is worth noting that the principal of separation of duties not only relates to key internal election management responsibilities, but also to external roles such as formalized oversight, audit and testing functions, decryption key possession, and quality assurance functions.

It is not clear if, and to what extent, some of the examples of Internet voting implement a separation of duties, although it is clear that most do to some extent. The French system, for example, has the role of the independent expert and a diverse representation on the Electoral Bureau tasked with implementing Internet voting. The Estonian system is subjected to testing by other public bodies and IT experts, and the EMB employs an external auditor.

The Norwegian system distributes a number of key components of the Internet voting system between organizationally independent institutions. Voter authentication portals are not administered by the Ministry. The vote servers are also maintained by different Ministries – one at the Ministry of Justice and the other at the Ministry of Industry and Trade. The servers on which the various stages of the counting and results process were conducted (cleansing, mixing, decryption and tallying) were controlled by the Ministry, but these steps of the process were conducted under the full supervision of election stakeholders. The encryption key is divided amongst political parties and a number of audit mechanisms are established and conducted by different entities, some entirely independent of government institutions.

Enabling Vote Updating36

The secrecy and freedom of the vote is one of the most serious challenges created by voting from uncontrolled environments. Internet voting systems need to ensure that vote secrecy is maintained and the challenges of voter coercion and vote buying are mitigated. One measure that can be implemented to deal with these challenges is the possibility for vote updating, sometimes called repeat voting. With this measure, Internet voters are free to cast Internet votes as many times as they wish to, and only the final Internet vote is included in the count. A further aspect of vote updating can allow Internet voters to also cast a paper ballot, either during an advance voting period or on Election Day. The paper ballot, cast from a controlled environment,[37] takes precedence over any Internet votes cast. The possibility for vote updating will mean that even if a voter is forced to vote in a certain way, the coercer will never know if that coerced vote is the one that was included in the count. This will remove the incentive to coerce voters or buy votes.

Only Estonia and Norway have implemented vote updating. Estonia allows Internet voters to cast as many Internet votes as they wish during the Internet voting period, with the last one being included in the count.[38] The names of Internet voters in Estonia are removed from the list of voters provided to polling stations, so casting a paper ballot on Election Day is not possible for Internet voters.

Norway implemented a similar system with a few additional features. Norway has an extended period of advance voting during which paper ballots can be cast in a limited number of locations. Internet voting runs in parallel to this advance voting period and any paper ballot cast in this advance voting period will take precedence over any Internet ballot cast by a voter. Furthermore, Internet voters always have the possibility to cast a paper ballot on Election Day, with the paper ballot taking precedence over any Internet vote.

Enabling Verifiability

One way to enable trust is to implement systems which independently verify the correct functioning of the system. Such verifiability can be either individual or universal in nature. Individual verifiability allows individual voters to check that their vote has been properly counted. Universal verifiability conducts independent checks on a systemic level to show that the calculated result is correct (Pieters 2006). Individual and universal verifiability rely on cryptographic proofs to demonstrate the correctness of the system. Both types of verifiability rely upon the initiative of the citizens. Given that they are independent of the electoral authorities, they are very useful tools to enhance citizen confidence in electoral processes.

While paper-based voting systems cannot be subjected to such cryptographic proofs of correctness, not utilizing cryptography in the voting process, they can be seen as verifiable in other ways. Transparent electoral procedures allow any observer to verify that the ballot box is empty at the beginning of voting;

[36] This measure is predominantly one that ensures the secrecy and freedom of the vote. However, it can be argued that it has some trust enhancing aspects. It is also included in the paper by Spycher et al (Spycher, Volkamer and Koenig 2011) and is therefore also included here.

[37] And therefore free from coercion and with no possibility for the voter to prove how they voted.

[38] Unless a paper ballot was cast during the advance voting period, in which case this vote is counted and all internet votes from this voter removed from the count.

it is sealed during the voting period; only entitled voters are inserting ballots only one time; ballots are adjudicated correctly; and each ballot is counted once. All these features guarantee the secrecy of the vote and ensure that the system is implemented correctly. Voters know their ballots are in the ballot box and counted, but nobody can identify which is his/her ballot.

However, traditional paper-based elections also include some features based on indirect verification means. Postal voting is the most evident case. Citizens who cast their ballots by post actually lose the chance to directly verify the electoral procedures. They trust other people (i.e., postal staff) to properly handle their ballots. A similar situation occurs in countries where only a handful of selected people (e.g., party representatives) are allowed to attend the final tally. The average citizen will lose his/her power to directly verify the tally and will have to have to trust other stakeholders in this oversight role.

The use of voter verifiable paper audit trail (VVPAT) is a key element within the on-going electronic voting debate (Norden *et al* 2007), but there are different approaches depending on which sort of electronic voting solution is in use. While VVPAT is accepted in non-remote voting machines in order to compensate for their lack of transparency[39], Internet voting does not generally use this mechanism because it cannot provide the same guarantees achieved for non-remote voting machines.

It is worth noting that this is an area where electronic voting standards and general electoral standards are somewhat contradictory. If a voter can prove to themselves through a verifiable system that their vote and its value have been included in the count, this opens the door to vote-buying and voter coercion. In other words, the standard of transparency runs contrary to the secrecy of the vote. Clearly these issues are complex, with competing demands and different countries finding different balances between the demands for strong verification and audit mechanisms (i.e. greater transparency) and secrecy. Some of the solutions to these conflicting demands are technically complex in nature and have been more prevalent in later iterations of Internet voting systems. Pieters and Becker argue that for Internet voting, the need for transparency (through verifiability) supersedes the need for absolute vote secrecy, especially as people are voting from unsupervised environments anyway. They accept the failure in vote secrecy as necessary to implement verifiable Internet voting (Pieters and Becker (2005): 11). However, others argue that the secrecy of the vote is of greater concern than transparency.

Emerging international standards seem to reject the use of voting receipts for Internet voting. A recommendation by the Council of Europe specifically precludes such receipts: “a remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast” (Council of Europe 2004: Recommendation 51). Despite these important barriers, some Internet voting solutions have included different types of receipts that intend to provide better verification means without breaching democratic electoral principles.

[39] Regarding non-remote voting machines, VVPAT has been increasingly introduced as a supplementary guarantee because it allows recounts of the paper audit trail in order to compare electronic results with paper-based ones. However, VVPAT can be implemented in many different ways and it is not a problem-free solution. Usability, for instance, might become a great concern because sometimes the receipts are difficult to manage and read. Moreover, some machines include these receipts with a ballot box embedded, where the voter cannot manipulate them, but others print out a paper trail which the voter has to insert into a separate ballot box. Beyond the layout, the actual use of these receipts may also be problematic. While some countries do not foresee an *ex officio* recount, others systematically conduct parallel tallies with statistical samples.

One solution consists of a receipt that does not include the content of the vote, but allows a partial check of the correct performance of the Internet voting application. After casting their ballots, voters receive a code and, once the election period is finished, the electoral authorities publish a list of received codes. Voters can check their codes on the list and consequently prove that their ballots have been received, though there is no evidence regarding their content or whether they have been included in the final tally. The code only proves that a given ballot has reached the cleansing stage, but it provides no evidence regarding whether it is included into the counting phase. Scytl, for instance, used this sort of receipt in certain Internet voting systems and it is one of the main features of its *Pnyx* application (Scytl 2005: 16-18).

A second solution provides the voter a so-called technical vote, an encrypted code given immediately after casting the ballot. Once the poll period ends, the election authorities publish a list of used codes that, in contrast to the previous solution, will indirectly link each code to a given candidature. The Dutch Rijnland Internet Election System (REIS) system used such a scheme. Obviously secrecy concerns may arise in this case because, "if a voter . . . discloses his authorization code and his technical vote, anyone can determine his/her actual vote by simply trying all the candidate identities until a match is obtained" (OSCE/ODIHR 2006: 15; Jones 2007: 20-25).

E2E verification mechanisms, such as that provided by the Dutch REIS system, can present other challenges in addition to the potential for violating the secrecy of the vote. The realization of E2E systems may be based on a number of assumptions and preconditions; that is to say they will only be able to correctly achieve their goals provided the voting system is being handled in a given way and with some specific features (Jones, 2009: 2-3). Such disclaimers should be seriously taken into account because they could undermine the usefulness of an E2E verification tool.

In terms of international practice, four cases of Internet voting include no means for voters to verify either that their vote was cast as intended or counted as cast (Canada-Markham, Estonia, Spain-Barcelona and Switzerland-Geneva). Three cases include a mechanism for the voter to prove that their vote was included in the count, but not to prove the recorded value of that vote (Australia, France and the UK).

The REIS system implemented in the Netherlands was unique amongst the cases of Internet voting in that it offered E2E verification. Before the elections, a pre-election reference table was published which contained all possible valid votes represented by key-less hashes together with a mapping to the corresponding candidates. During the election, the votes cast by legitimate voters built a post-election table where the votes were represented by hashes made using the voter's secret key. The outcome of the election was calculated by computing key-less hashes of each vote in the post-election table. If the vote is valid, its hash value can be found in the pre-election table and the chosen candidate can be determined. And since this hash is a key-less hash anyone can compute it, hence anyone can check the result of the election.

In addition, at the end of the voting procedure the voter received a "technical vote" and a control value (code). Each voter could verify whether his vote has been taken into account and how (which value) by looking at the table of preliminary or final results posted on the Internet. The Organization for Security and Co-operation in Europe (OSCE) noted its opinion that, “designers of RIES have effectively opted to surrender protection against coercion of a voter in favor of greater transparency” (OSCE/ODIHR 2006: 15).

The Norwegian system considers itself to have E2E verifiability, but has implemented this with several novel features, which can be seen to deal with some of the challenges outlined above. On the completion of each voting transaction the voter is sent a return code. The return code is sent to the voter’s mobile phone and consists of a number relating to the political party that they have cast a vote for. The codes for each political party are printed on the reverse side of the voter’s polling card (sent to the voter before the election), but on the inside of their sealed polling card.[40] Each voter has a unique set of codes for the political parties running for election. Therefore, by matching the return code with the codes printed on the back of the polling card, the voter can verify that the vote has been cast as intended.[41] Moreover, as there is the chance to cast repeat Internet ballots or paper ballots, return codes would not be seen as evidence that might endanger the secrecy or freedom of the vote.

The voter has no proof that the vote has been stored as cast, or counted as cast, and the Norwegian system makes no attempt to provide this verification on an individual level. Instead the correctness of the system is verified on a system level through the conduct of several quality assurance mechanisms conducted by independent experts. Checks were made that each of the database of votes used for the counting process corresponded to the votes stored on the vote server. Custom made software was developed to verify the identity of the hashes generated by the Return Code Generator (RCG) with the hashes to be calculated from the votes stored by the Vote Collector Server vote server. This proved that the vote server had not removed any votes that the RCG had registered.

In addition to this, independent mathematical proofs were verified to assure the integrity of three key stages of the counting process. Firstly, it was verified that the result of the cleansing process did not contain any votes not included on the vote server. Secondly, a check was made that the votes entering the mixing process were correctly output from the mixing process. Finally, a check was made to ensure that the correct private key was used to decrypt the votes. The proofs were verified independently using software by an external organization[42] working closely with the internal auditor of the software from the supplier. They verified these stages of the process using zero-knowledge proofs (Vollan 2011: 7-8).

The combination of these individual and universal verification mechanisms are seen as providing overall E2E verifiability in a way that does not violate the secrecy of the vote because of the possibility to cast repeat Internet votes and can always cast a paper vote.

[40] The polling cards were perforated and codes only visible after opening.

[41] This system of return codes also deals with the secure platform problem for internet voting.

[42] The verification of these stages of the vote counting process was open to anyone to conduct, and the Ministry had hoped that an organization(s) would conduct this verification independently. When no organization indicated its intention to do so, the Ministry contracted Promis AS to conduct this external verification.

Evaluation

Decisions by electoral stakeholders to trust an Internet voting system are rational ones based on the evidence available to these stakeholders. Elections are required to meet certain standards if they are to accurately reflect the will of the voters. Conducting an evaluation of the extent to which Internet voting systems meet electoral, and other, standards can help to provide stakeholders with the evidence needed to enable trust in those systems. Spycher *et al* suggest that Internet voting systems should be assessed against standards including, "formal voting protocol analysis, Common Criteria, ISO 27001, the k-resilience value, process observation, and usability standards" (Spycher, Volkamer and Koenig 2011: 9). Internet voting systems should certainly be measured against this set of standards, but should also be assessed against more general electoral standards, as defined in public international law. These standards are rooted in the Universal Declaration of Human Rights and the International Covenant of Civil and Political Rights and have been clarified and elaborated by international organizations.[43]

In addition to the general electoral standards, the growing use of election technologies has led to the embryonic development of electoral standards for the conduct of electronic voting, including Internet voting. However, these standards are still emerging and even the most comprehensive of them, the Council of Europe's E-voting Recommendation (Council of Europe 2004), is only a recommendation and therefore not binding for members of the Council of Europe. Furthermore, it is only a document agreed on by members of the Council of Europe and has even less legal authority outside of the members of the Council. It is also worth noting that the standards developed so far have been largely developed with electronic voting and counting machines in mind. While these emerging standards are relevant for Internet voting, standards specifically directed towards remote voting may be necessary in the future in order to adequately deal with the challenges related to remote voting, including Internet voting.

There is little information publically available about other countries' assessments of Internet voting systems against the various standards. It is likely that in fact few of the systems have actually been comprehensively assessed against these standards. There are a number of possible reasons for this. Several of the Internet voting systems have been developed for pilots and such assessments are less likely for pilot systems. Some of the standards are also relatively new (e.g., the k-resilience test) while electronic voting standards are still at an embryonic stage.

The Norwegian Internet voting project has attempted to measure its Internet voting system up against some of these standards. As part of the formal evaluation process for the Internet voting project, one of the assessment areas relates to the compliance of the system with international electoral standards, specifically the Council of Europe Recommendations. This assessment topic, which is being conducted by IFES, will also look at the more general electoral standards, as well as electronic voting standards which may be emerging from other key electoral organizations. A further area of assessment concerns the accessibility of the Internet voting system. This part of the assessment will be conducted by ISF and will look at accessibility issues in general as well as usability issues for voters with disabilities.

[43] Such as the United Nation, the Organization for Security and Co-operation in Europe, the European Union, the Organization of American States, the African Union, the Council of Europe and the Inter-Parliamentary Union

The Norwegian Internet voting system was also required to be certifiable to Common Criteria Evaluation Assurance Level (EAL) 2[44] for administration and scanning and 4+ for Internet voting and distribution of seats. While the system was required to be certifiable to these standards, the Steering Committee for the Internet voting project decided that the system would not be certified prior to the pilots, only if a decision is taken to implement Internet voting on a broader scale. Ensuring certifiability of the system will become part of the acceptance testing for the system.[45]

The Ministry did require that the supplier(s) of the Internet voting system are certified to, or work according to, ISO 27001. The supplier's compliance with this standard has been part of the scope of work conducted by Veritas, who are doing a quality assurance audit for the project. The Ministry has also contracted an independent IT consultancy to conduct a k-resilience test for the system, but at the time of writing the results of this test are not available.

Test Elections

A final mechanism that can play an important role in enabling trust in Internet voting systems is the conduct of test elections. This allows voters and other stakeholders to experience the full Internet voting experience before the system is used for binding elections (Spycher, Volkamer and Koenig 2011: 10). This trust mechanism is also part of the Council of Europe's Recommendations, which states that, "Voters shall be provided with an opportunity to practice any new method of e-voting before, and separately from, the moment of casting an electronic vote" (Council of Europe 2004: recommendation 22).

Few countries appear to have met this Council of Europe recommendation by offering all voters the opportunity to use Internet voting systems in test elections prior to their use in binding political elections. One example of a country that did do this is Switzerland-Geneva, which has a website in a range of languages for voters to test out voting over the Internet.[46]

Norway met this requirement of the Council of Europe in a number of ways. It used the Internet voting system in trial ballots in each of the pilot municipalities in the 12 months preceding the local government elections. These ballots were for youth councils and for local consultations. Not all of the features of the Internet voting system were available in earlier trials, but later trials used the full functionality of the Internet voting system, including return codes. Obviously not all voters in the pilot municipalities would be eligible to participate in youth council elections. However, voters in the pilot municipalities were also provided the opportunity to experiment with the Internet voting platform through a test Internet voting website established by the Ministry. This website was an authentic copy of the actual Internet voting website, including the use of third party authentication mechanisms (such as the MinID portal) and return codes, and was available from July 20 to August 1.[47]

[44] There are seven levels of assurance for compliance with the Common Criteria, with level one being the lowest level of assurance and seven the highest. Level two required that the system has been structurally tested. Level four requires that the system has been methodically designed, tested and reviewed.

[45] Information provided by the Ministry in email dated January 3, 2012.

[46] See http://www.ge.ch/evoting/english/welcome.asp [last accessed on February 29, 2012].

[47] The test website did not have the proper political party names.

Conclusion

As can be seen from the preceding discussion, trust is a complex issue, especially in the context of Internet voting. However, it is an issue that needs to be taken very seriously by election administration bodies considering the use of electronic voting technology. Failure to do so can have devastating consequences for the legitimacy of the electoral processes, and even lead to failed technology projects costing many millions of Euros.

A number of trust-enabling mechanisms in the context of internet voting have been discussed above. It is important to note that as Spycher *et al.* state, the mechanisms used to enable trust are complex, can be difficult to enact, and can entail significant extra cost and complexity for any internet voting project. Furthermore, it is not the case that all of the mechanisms need to be implemented (Spycher, Volkamer and Koenig: 10). They are all mechanisms that can enable trust in the system, but may not all be required to obtain an acceptable level of trust. They can be seen as a menu of options for obtaining the required level of trust, and some may be more or less achievable/appropriate in the particular circumstances related to an Internet voting system or electoral environment. However, the more of these mechanisms that are implemented, the higher the level of trust is likely to be in any Internet voting system.

It is clear that the Norwegian Internet voting system has gone to considerable lengths to implement measures that enable trust in its Internet voting system, more so than any other example of Internet voting.

Secrecy and Freedom of the Vote

Internet voting is not only an external and cosmetic modification of electoral procedures; it also entails some challenges that are directly linked to fundamental electoral and democratic principles. This section of the report will discuss features of Internet voting that generate concerns regarding the protection of the secrecy of the vote and the freedom of the voter.

First the concept of ballot secrecy will be explored, tracing the origins of secret ballots to the evolution of the current Australian ballot which is used extensively around the world as well as exploring different interpretations of what is required in providing a secret ballot. The use of Internet voting presents some significant challenges in ensuring ballot secrecy. These will be evaluated before the report discusses ways in which other Internet voting countries and Norway have sought to mitigate these challenges to ballot secrecy. Finally, some conclusions will be drawn in general about Internet voting and ballot secrecy, as well as the Norwegian solution to this challenge.

Meaning and Importance of Secrecy of the Vote

Secrecy of the vote is enshrined in every international electoral standard, like Article 3 of Protocol 1 to the European Convention on Human Rights, but it is not a self-evident principle. The link between democracy and this kind of secrecy is not obvious. Secrecy entails some disadvantages like potential privatization of public affairs. Therefore its implementation should only be accepted after a nuanced consideration of advantages and drawbacks has been made.

Normally secrecy of the vote is conceived as an easy way to dissuade intimidation, bribery, and other similar coercion of the voter. If the vote remains secret, voters will have no chance to prove that they followed the instruction of a coercer and, given this impossibility, the coercion itself becomes meaningless. Voters will therefore be free to vote in a manner that expresses their own political choices, and not those of others. Although undue influences might be initiated from many sources, family voting is a significant concern in some countries; that is to say, the coercion's origin is located within a group of relatives.

From this point of view, secrecy somehow is a sub-principle intended to help achieve the freedom of the vote, and this freedom actually becomes the main goal for this understanding of democracy, only based on the aggregation of individual choices. However, other peoples (e.g., some indigenous communities) prioritize different democratic frameworks where the individual approach has to be balanced by communal needs. This collective understanding of public affairs could also have some impact over the importance of the secrecy of the ballot and actually is the main driver of on-going debate regarding the Australian ballot.

Brief outline of the Australian ballot debate

The term “Australian ballot” refers to two developments in the conduct of elections. The term is generally used to indicate the move from voting through a show of hands in public meetings to the use of paper ballots cast in private polling booths. However, it is also indicative of the move from independently printed ballot papers, to the production of standardized printed ballot papers by electoral authorities. Both measures were intended to ensure that voters were able to cast their ballots free from coercion so that electoral results better represent the will of the people.

Although almost all national electoral laws include secrecy of the vote as a main legal principle, the introduction of the Australian ballot was only accepted in Europe in the late 19th century and there was (and still is) an important theoretical debate on the convenience of adopting it. Right now some authors still claim that a public ballot is the only way to ensure a mature approach to public affairs because each voter’s choice would be somehow modified by other citizens. This mutual supervision would create a collective understanding of public affairs, and citizens will no longer cast a ballot based only on egoistic self-interests.

A number of voices have spoken out against the Australian ballot in the last two centuries. John Stuart-Mill probably is the most well-known and he added some specific arguments to this debate (Buchstein 2010: 17-26). He understood the right to vote both as an individual as well as collective action. Given that voters cast their ballots assessing which are the general needs, voters cannot be the primary owners of this franchise. They would only be using a faculty that has been given to the whole citizenry. Therefore casting a ballot is obviously a right, but also a civic burden and not something that can be exercised from a personal perspective alone.

Although western democracies closed this debate backing the Australian ballot as a means to guarantee the freedom of the vote, the theoretical debate is still alive. Brennan and Petit, for instance, argue that bribery and blackmail are also feasible with secret ballots, but they admit that social intimidation would increase if public ballots were implemented (Brennan and Petit 1990). They conclude by accepting secret ballots. However, they emphasize that, from a democratic point of view, what would be desirable is a public ballot system due to its advantages for a deliberative democracy – a step further from an individualistic political system.

The secrecy of the vote: obligation to ensure or obligation to provide the opportunity

Once it is accepted that the secrecy of the vote cannot be ignored, there is still a supplementary question as to what are the specific commitments that electoral bodies should meet in this regard. Some stakeholders think that public bodies should only need to provide the option to cast the ballot completely alone and it would be up to the voter whether to use it. As Wolfgang Drechsler recalls, this argument was used by Estonian authorities during the initial debates:

> *"To start from the assumption that the State must 'trust the people' and not interfere if at all possible in any of their decisions ... As an example in our context, the problem that e-voting would facilitate some families, friends or colleagues voting together, i.e. practice collective voting, as well as the buying and selling of votes, was said to hinge on the question of whether the State would have to protect an individual only from other individuals or also from her- or himself. It was not seen that collective voting could be a problem for the state as well, and not only for the individual." (Dreschler 2004: 13)*

The Estonian Supreme Court, for instance, also backed this trend when it recalled "the obligation of the state to guarantee the protection of voters against the persons who try to influence the voter's choices. Pursuant to this principle the state must create necessary conditions for conducting free voting and protect voters from such influences that prevent the voter to give or not to give his or her vote in the manner he or she wishes." (Estonian Supreme Court 2005: § 27)

As analyzed below, this reasoning did not lead to a refusal of Internet voting because this public commitment might be met by providing alternative voting channels that ensure the secrecy of the vote. It would be up to voters to decide which channel best suits their needs.

There is also another option that underlines that what is pursued by the secrecy of the vote can only be achieved if it is understood as a universal commitment that public bodies should consider as being compulsory for each voter. The protection of the secrecy of the vote should not be transferred to each voter. Assuming that voters might be submitted to undue influence that violates their freedom to vote, the best solution would consist in only admitting those ballots cast alone. It would also be a universal measure so that everybody would be subjected to such conditions regardless of particular conditions.[48]

However, if this approach is understood in a broad way, it would lead to rejection of all remote voting channels, both with electronic or paper based means, and such a conclusion will ignore that many countries are already admitting at least paper based remote voting, that is to say, postal voting from unsupervised environments.

[48] See also how End-to-End (E2E) verification tools might impact these different meanings of the principle of secrecy and which legal challenges (Jones 2009).

The Challenge of Internet Voting for Ballot Secrecy and Freedom of the Vote

Unsupervised environments cannot guarantee that voters cast their ballots alone

Internet voting can be used both from supervised environments (e.g., Finland) and unsupervised environments (e.g., Estonia). How to protect the secrecy of the vote and freedom of the voter is probably the main difference between Internet voting in both environments.

A polling station is meant to be laid out in such a way to mitigate any attempt to influence voters when they are casting a ballot. Voting booths, the supervision of an independent polling board and the procedure itself, from authentication till voting, are thought to generate an appropriate framework to cast a ballot free from external influence and also guarantee the principle of secrecy.[49]

Although there are exceptions (e.g., Spain), using voting booths for traditional paper ballots in a polling station is normally compulsory for voters. This is a crucial requirement since it might be the only moment when voters are alone and, therefore, protected from any undue influence and able to freely decide how to cast their ballot. It must be noted that new communication technologies may weaken this protection since mobile devices might be used by voters in order to record evidence of how they have voted. The voter may take a picture of the ballot after it has been completed so that the voter can prove to a coercer that the voter has followed the coercer's instructions. This ballot can obviously be invalidated after taking the picture and a replacement ballot completed differently, but a significant number of invalid ballots could raise a coercer's suspicion. Moreover, if the instructions lead to somehow customizing the ballot, invalidating the ballot afterwards would not work.

It can be argued that such strategies can only be implemented on a small scale because social barriers will make massive intimidation of voters unlikely without being widely known. However, these social barriers will not have the same strength in all countries and, at least from a theoretical point of view, election law should take into account all these breaches, even if there are only a few. After all, some electoral contests are very close, and even one vote can change an election.

Once the ballot has been filled in, traditional polling stations also provide a layout that serves to protect the secrecy of the vote and allow observers to verify the integrity of the process. Assuming that electoral procedures in polling stations are open to observation, any observers should be able to verify that the ballot box is empty at the beginning of voting, sealed during the voting period, only entitled voters are inserting ballots and only one each time, that each ballot is counted once and, finally, that ballots are counted correctly. Moreover, specialist knowledge, such as computer science, is not needed to understand the process. Even illiterate people are able to verify its correctness and whether fraud has taken place in the polling station.

This perfect world of observation in polling stations is far from reality. Electoral stakeholders often do not use all the chances for observation and scrutiny offered by the election system. Although observers are allowed to remain in the polling station during the voting period, there are often not enough observers or interested voters to provide complete observation in all polling locations for the entire

[49] See the ACE website for more details of the principles that should be followed in designing the layout of polling stations - http://aceproject.org/ace-en/topics/vo/vof/vof03/vof03a/vof03a02 [last accessed on February 17, 2012].

period of polling. In some cases, observers may show up only for the final tally. It is important to acknowledge that even in those countries where observation coverage is not complete it would always be possible to observe the entire proceedings in a polling station, and this has a deterrent effect regardless of the actual presence of any observers on Election Day.

On the other hand, unsupervised voting can never provide the same guarantees of secrecy and freedom of the vote. Therefore, unsupervised voting generates concerns about how to protect these core electoral and democratic principles. A classical paper of Brennan and Petit (1990), who actually disagree with the secrecy of the vote, argue that unsupervised voting scenarios might lead to bribes, blackmail and social intimidation. Given that voters cast their ballots within a private and unsupervised environment, there will be no one able to protect against undue influence and therefore third parties could freely approach voters to try and buy their votes. In short, voting from unsupervised environments cannot guarantee the secrecy of the vote and this opens up the possibility for the coercion of voters and vote buying, practices which run contrary to fundamental democratic and electoral principles. Brennan and Petit argue instead, at least from a theoretical basis, that an open voting process would be better if social intimidation did not exist (Brennan and Petit 1990).

Authentication data and the vote's value should remain separated

Internet voting is a form of remote voting, which means that since authentication data and voting data have to be communicated, often using the same channel, there is an obvious danger of maintaining the link between voter identification data and the value of the vote. It is easy for Internet voting used within supervised environments to split both data since authentication can be carried out by traditional means (e.g., exhibition of an ID credential to polling staff) and, once verified, the voter can remotely cast a completely anonymous ballot.

Taking this framework into account, it should be noted that secrecy means freedom when it is understood by voting alone, as we have already seen, but it also means anonymity when applied to procedures to be handled after casting the ballot. While paper-based ballot boxes protect the anonymity of the ballot by physically separating the authentication and voting processes, Internet voting generates serious concerns about how to achieve the same goal. Once the ballot is sent, it will remain stored in so-called “voting servers,” that is to say, computers linked to a computer network that will receive the electoral data during the voting period. Such servers will store these data even when the ballot has been canceled by electronic or paper means. Given that these servers will need to store both ID credentials of those having voted and the content of votes cast, only computerized means may avoid that someone is able to link both data. Such innovations mean that the process of making votes anonymous, and subsequently the principle of secrecy, rely upon technical measures that an average voter is unlikely to be able to understand, since specialized knowledge is required.

Normally a cryptographic system based on a two-envelope layout is used to avoid linking voters with their votes. As in traditional postal voting, the outer envelope will only include the ID credentials and the inner one the actual ballot. Both envelopes will be protected by digital signatures and key management protocols will avoid their improper manipulation during the polling period. At the end of this stage, the outer envelope will be used to verify whether each voter is entitled to cast a ballot and afterwards both envelopes will be split. Inner ones will then be submitted to a mixing procedure in order to destroy any sequential data and finally they will be decrypted.

Hacking is always a major concern with Internet voting projects, namely with those devices that are not directly and permanently controlled by election authorities. The voter's personal computer, the transmission channel or even the applet, that may be used to provide the voter with an original ballot, might be the object of attacks. It is worth noting that secrecy will be breached when such attacks manage to unveil the ballot and read its content. It is not necessary to alter its value or even delete it. Actually the voting procedure could normally continue and, if IT devices are not correctly setup, elections authorities could even not notice that someone has previously inspected the ballot.

Solutions Provided by Countries using Internet Voting

This section will analyze different approaches to the challenge of secrecy and freedom of the vote adopted by those countries using Internet voting mechanisms. Each one approaches this problem with interesting nuances that feed the overall debate with practical inputs.

Internet voting is assimilated to postal voting

Internet voting is not the only way to remotely cast a ballot since, as mentioned, many countries are using traditional postal means. Many of the concerns raised by Internet voting are very similar for postal voting. Both channels are based on voting from unsupervised environments and such environments cannot provide the same guarantees of secrecy and freedom as are commonly implemented within polling stations. Briberies, intimidation and other similar coercions are more likely to happen and also the principle of secrecy might be endangered both by Internet and by postal means.

Despite these known dangers, the use of postal voting is not seen as contrary to international electoral standards under certain conditions. The Venice Commission's report on this specific issue of remote voting, that includes Internet voting, postal voting and any ballot cast from non-supervised environments, finds that such voting complies with European electoral standards. After providing comparative data on this issue, the Venice Commission concludes that:

> *"69. ... remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either non-supervised postal voting or electronic voting.*
>
> *70. In addition, for non-supervised e-enabled voting, technical standards must overcome different threats to those which exist for postal voting. This form of voting must only be accepted if it is secure and reliable. In particular, the elector must be able to obtain confirmation of his or her vote and, if necessary, correct it without the secrecy of the ballot being in any way violated. The system's transparency must be guaranteed. Insofar as an e-enabled voting system meets these conditions, it is compatible with the European standards on electoral matters, and in particular with Article 3 of Protocol 1 to the European Convention on Human Rights."* (Venice Commission 2004)

Once remote voting is accepted as a legitimate channel to cast a ballot, it is worth noting that postal voting may also be implemented in different ways with different impacts on electoral principles. For instance, in Spain postal voting is allowed, but voters can only cast their ballots through recommended mail. That is to say, they have to show up at a postal office, identify themselves (only recently) and insert their ballot in a special envelope. Although this protocol does not provide the same guarantees as a traditional polling station, it intends to implement some degree of protection for postal voting. However, other countries allow postal voting in a more flexible way. In Switzerland, for instance, voters can cast their ballot by inserting the polling card that they have previously received in a normal postal box located in any street. Ordinary mail, with no supplementary mechanisms of control, is used even for electoral material.

Taking into account the Geneva example (similar to many country's use of postal voting), Internet voting does not seem to increase the concerns already seen in this sort of postal voting. From the perspective of how these voting channels meet the principle of secrecy, both internet voting and fully unsupervised postal voting have the same risks. While internet voters might be forced to show the value of their votes, the same undue influence might be received by voters who cast their ballots in a normal postal box. Moreover, while the internet ballot might be read by intruders, the same is also possible for paper ballots inserted into postal boxes.

Countries adopting internet voting often do it for similar reasons as they offer postal voting, namely to facilitate the participation of certain voting groups (e.g. impaired people, citizens living abroad, etc.). The state of West Virginia, in the United States, sought to assist overseas voters to participate; France similarly with its *Assamblée des Français à l'Étranger* and Australia sought to enfranchise people with disabilities. All saw Internet voting as a means to increase the turnout of a group of citizens that normally face significant barriers to casting ballots. These three countries previously used traditional postal means and therefore the introduction of Internet voting might not generate more concerns from our current point of view. In Norway, postal voting is also allowed for Norwegians living abroad as a way to ease their political participation.

In conclusion, postal voting and Internet voting face similar dangers. If the former is accepted then there seems little reason to reject the latter, at least using a similar set of arguments. Moreover, if the previous rate of postal voting usage is very high, as happens in Geneva, the implementation of Internet voting could be seen as a natural update of voting channels.

Internet voting provides the option to cancel a cast ballot by electronic and paper means

As we already know, voting from unsupervised environments cannot guarantee that voters are casting their ballot alone and without undue influences, but the secrecy of the vote might not be breached if only the voter knows which ballot is the one that will be counted by the electoral authorities. If the voter can always revoke a vote, third parties will never be sure that the ballot cast in front of them and under their influence is the actual one counted. Following the Estonian Supreme Court:

> *"…the voter's possibility to change the vote given by electronic means, during the advance polls, constitutes an essential supplementary guarantee to the observance of*

> *the principle of free elections and secret voting upon voting by electronic means. A voter who has been illegally influenced or watched in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again either electronically or by a ballot paper, after having been freed from the influences. In addition to the possibility of subsequently rectifying the vote given under influence, the possibility of voting again serves an important preventive function. When the law guarantees a voter, voting electronically, to change the vote given by electronic means, the motivation to influence him or her illegally decreases. There are no other equally effective measures, besides the possibility to change the vote given by electronic means, to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium. The penal law sanctions do have their preventive meaning but subsequent punishment - differently from the possibility of changing one's electronic vote - does not help to eliminate a violation of the freedom of election and secrecy of voting." (*Estonian Supreme Court 2005: § 30)[50]

Accepting this means that the secrecy of the vote should always be understood as a subjective guarantee. While the value of a vote may be disclosed due to external coercion, this fact becomes meaningless if nobody is able to assess whether this vote actually is the valid one. From a factual point of view, the secrecy of the vote might have been breached, but, from a subjective perspective, nobody can take advantage of this information because other votes may be valid. Electoral law would admit this subjective meaning of secrecy and therefore Internet voting would meet this criterion provided it allows multiple voting.

In Estonia, voters can repeat their votes multiple times and the tally would only include the final one cast by electronic means, or the one cast by paper within a traditional polling station in the advance voting period. Internet voting remains active during an advance electoral period that finishes 48 hours before Election Day. If the electoral system also admits an advance period for paper based means, which does not happen in Estonia, the chances to revoke a vote are increased, as either paper or electronic means can be used to do this, either during the advance period or during Election Day (as is the case in Norway).

Beyond the solution adopted by Estonia and Norway, it is worth noting that the revocation of votes has some procedural and legal consequences that should be considered. While it might address concerns linked to the principle of secrecy, it is also true that the revocation creates a new burden for voters who aim to protect the secrecy of their vote. Traditional procedures ensure secrecy without any additional measures on the part of the voter, but now this citizen might have to vote at least twice to guarantee the same legal principle. Moreover, normally these solutions do not foresee a complete revocation; that is to say, they admit a substitution of the vote, but the voter could have been forced to vote when their

[50] See also Drechsler who recalls how this argument was already used during the very first debates regarding the implementation of internet voting (Drechsler 2004: 11-17).

preferred option was not to vote at all.[51] The vote can only be substituted and not completely canceled, although some countries do allow the casting of a blank ballot by the Internet.

Internet voting only as a supplementary voting channel

The protection of the secrecy of the vote is understood as an option for the voter and this commitment of the public authorities is met by providing a voting channel with supervised environments and voting booths. It is worth recalling here that almost every Internet voting project is somehow relying upon this argument, provided it foresees different voting channels. Estonia and the relevant Swiss cantons use both electronic and paper means, and Internet voting can be seen as an option offered to those citizens that, for any reason, prefer this system to another one that better protects the secrecy of the vote.

The referendum held in Barcelona in 20ten also follows this approach. There was no postal voting and, although technically feasible, legal regulations did not foresee a way of revoking or replacing votes. Therefore, the only way to address secrecy concerns consisted of emphasizing that voting from an unsupervised environment was the free decision of each voter because the organizers also deployed a network of supervised Internet polling stations.

Internet voting technically guarantees that the system does not reveal the votes' value

As mentioned before, the secrecy of the vote can also be breached if it is not anonymous and the content is revealed to third parties after casting the ballot. Traditional polling stations provide this guarantee with sealed ballot boxes and supervision by electoral officials, political representatives and electoral observers. Remote voting, either electronic or postal, cannot provide this secure framework since the ballot will have to travel through different routes that do not have the same levels of supervision, and, in fact, in which supervision may not be possible at all.

Postal voters, for instance, will have to trust postal officials because they will handle the ballots and transport them to the relevant polling station. Secured ballots, like those that include anti-tamper measures, may dissuade certain manipulations, but they cannot totally avoid them. Therefore, beyond the actual deficiency of postal services, that used to be another major barrier for this voting channel, the probity of these postal officials would always be a key element for its correct implementation. There will be no political representatives or electoral observers to supervise these steps and the system will have to rely upon other measures; in this case, confidence in the postal services, either national or even foreign ones if voting from abroad is admitted.

Internet voting faces similar problems and, although using different means, the solution shares the same logic for postal voting. The ballot remotely cast by electronic means will have to travel through the Internet to reach the voting servers that assume the role of ballot boxes during the election period. This trip is somewhat similar to the one made by postal ballots, although, in this case, postal means will be substituted by electronic means. However, the challenges are the same because both channels will not have the same level of supervision that normally exists in polling stations or, in this case, for the electronic ballot boxes. While postal voting relies on postal officials, Internet voting must do the same

[51] Although casting a blank vote is possible in many countries.

for computer experts, since only computerized means may guarantee that the ballot is stored as cast without revealing its value to anybody.

Each country has its own solution and, beyond what is already said regarding the use of double envelopes, cryptographic procedures and mixing operations, this section does not intend to develop a technical review of such options. It is at least worth noting, however, that a main part of the principle of secrecy can only be ensured by computer means and therefore the way to independently supervise these electronic devices become strategic. While postal voting can only be admitted if postal services are able to achieve a given level of efficiency and probity, that would have to be somehow assessed; Internet voting will have to rely on computerized means that will also have to be assessed. The section devoted to transparency and integrity issues will analyze how to conduct such assessments in a plural and independent manner.

Conclusion

Secrecy is a significant concern in every electronic voting application. In the case of Internet voting from unsupervised environments, this principle may easily become the main challenge. Normally, secret ballots are seen as tool to protect the freedom of the vote, but it is always true that this solution is not cost-free. As stressed during the debate about the Australian ballot, it somehow fosters a privatization of elections so that voters may cast a ballot taking into account only their privative interests and not common goods.

Secrecy may entail at least two tenets. First of all, secrecy means that the voter should be able (required) to cast his/her ballot alone. Secrecy is thus linked to freedom. Second, secrecy also prevents third parties from knowing the vote of a given citizen once cast. Secrecy is, therefore, also linked to anonymity.

Given that an Internet voting system cannot ensure that voters are casting their ballots alone, potential solutions should be found in supplementary reasoning that will be used to justify Internet voting. Similarities with postal voting or the chance to repeat and cancel a vote are common arguments for the acceptance of Internet voting. To understand the principle of secrecy as a mere option is another strategy for Internet voting. The principle would only be met by providing a way to vote alone, but there can be other optional channels where secrecy is not ensured.

Finally, regarding anonymity once the ballots are cast, only computerized means are able to achieve this goal.

The Accessibility of Internet Voting

Accessibility of the voting process is an often-quoted reason for implementing electronic voting, whether in a polling station or in its remote form. Accessibility is indeed a topic of growing importance in the workshops and literature on the electoral process, especially in the Americas. The concept of "accessibility" is often used in conjunction with that of "usability."

According to Whitney Quesenbery, former president of the Usability Professionals' Association of the United Sates and former appointee to the Electoral Assistance Commission (EAC), "historically, usability (or human factors) has worked to maximize the number of people who can use a product without difficulty. Accessibility work has focused on minimizing the number of people who are unable to use a product at all, or can only use it with great difficulty . . . Usability and accessibility go hand in hand. Improving the accessibility of a product can improve its usability for everyone." (Quesenbery 2008: 1)

The concern with voting systems is for voters to be able to vote accurately. The draft U.S. Voluntary Voting System Guidelines say for instance: "The voting process shall provide a high level of usability for voters. Accordingly, voters shall be able to negotiate the process effectively, efficiently, and comfortably" (NIST 2009: 49). This echoes the definition of usability from ISO 9241-11, which defines usability as "ability of specified users to complete tasks in a specified context of use with effectiveness, efficiency, and satisfaction in a specified context of use."[52]

In the case of voting system standards, the "users" are the broad group of all voters, including people with disabilities (visually impaired people, people with reduced mobility, etc.) or those who speak other languages. Accessibility of voting systems is, therefore, not only a matter of making these systems user-friendly for disabled people, but also for "ordinary people", taking for instance into account language and cognitive issues. Usability of voting systems also deals with functions such as vote verification.

This section of the report will first look at what the accessibility standards are that Internet voting systems may be required to comply with. These standards are found in specific accessibility standards for voters with disabilities, general electronic voting accessibility standards outlined in the Council of Europe's Recommendations (Council of Europe 2004), and more general accessibility standards. The accessibility requirements that have been included in the project design for the Norwegian Internet voting system will briefly be discussed, before exploring various aspects of Internet voting accessibility. For each of the aspects of accessibility, both international experience from the three in-depth case studies of Internet voting and the Norwegian experience will be discussed.

Accessibility Norms and Standards

Disability Access Standards

In international law and norms systems, accessibility is first and foremost an issue of giving disabled persons access to all services (health, education, sport facilities, etc.) that are open to non-disabled people. Ultimately, accessibility is about the right of disabled people to a parity of opportunities with non-impaired persons. One finds mentions of the political rights dimension of accessibility in texts such as the United Nations Convention on the Rights of Persons with Disabilities[53]. Article 29 of this convention, dedicated to "Participation in political and public life" states that:

> *"States Parties shall guarantee to persons with disabilities political rights and the opportunity to enjoy them on an equal basis with others, and shall undertake . . . [t]o ensure that persons with disabilities can effectively and fully participate in political and public life on an equal basis with others . . . including the right and opportunity for persons with disabilities to vote . . . by . . . [e]nsuring that voting procedures, facilities*

[52] See http://www.usabilitynet.org/tools/r_international.htm [last accessed on February 29, 2012].

[53] See http://www.un.org/disabilities/convention/conventionfull.shtml [last accessed on February 29, 2012].

> *and materials are appropriate, accessible and easy to understand and use . . . [and] [p]rotecting the right of persons with disabilities to vote by secret ballot in elections and public referendums"*

The Convention entered into force on May 3, 2008. It was opened for signature on March 30, 2007, and 82 countries, including Norway, signed it on that day. This is the highest number of signatories in history to a UN Convention on its opening day. At the time of writing, however, Norway has not ratified this Convention.

Other sources, including customary law or codes of good practice, extend the explicit requirement for accessibility to the political process for a number of groups. These include: those unable to reach a polling station, the elderly, the illiterate, students, poll workers, conscripts, foreign-service personnel, eligible voters in hospitals, eligible voters currently out of the country, and prisoners who have voting rights (International IDEA 2002: 73, EISA 2003: 24, UN 1994: §110, Goodwin-Gill 2006: 126).

The Council of Europe Recommendation

The Council of Europe Recommendation on legal, operational and technical standards for e-voting (Council of Europe 2004), which Norway incorporated into its own legal framework for the Internet voting project[54], also deals with accessibility in 10 of its standards. The four most relevant recommendations are below;[55]

- Recommendation Nr 3: "E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities."
- Recommendation Nr 4: "Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting."
- Recommendation Nr 9: "The organisation of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.
- Recommendation Nr 63: "Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI)."

The Council of Europe recommendation links accessibility with universality and the personal exercise of vote, which are founding principles in international law regarding political rights. It states that electronic voting reinforces universality and may broaden access to unassisted voting if properly designed - providing the electronic channel is not the only one available to voters.

The electronic voting opening period does not need to coincide with that of traditional polling stations. E-voting systems must be conceived bearing in mind the constraints of voters (visual, linguistic, etc.) and of their IT system in the case of Internet voting. The World Wide Web Consortium (W3C) norms are the

[54] The regulation does exclude some of the Council of Europe recommendations from being applicable – numbers 25, 40-41, 49, 52 and 111-112 - http://www.lovdata.no/cgi-wift/ldles?doc=/lf/lf/lf-20110331-0355.html [last accessed on February 12, 2012].

[55] Council of Europe Recommendations 45, 61, 62, 64, 65 and 96 are also relevant.

benchmark as far as accessibility for disabled people is concerned. The way to achieve a high degree of user-friendliness is to involve users in the designing process of the system.

General Accessibility Standards

Standards for accessibility have been developed to implement the evolving legal requirements for accessibility. The ISO 9241-11 standard deals with ergonomic requirements for office work with visual display terminals. It is therefore not directly connected with the voting process, but derives its relevance from its prescriptions in the field of human-machine interaction. ISO 9241 defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

ISO 9241-11 defines a usability framework, which is the basis of the structured method for developing human-machine interfaces. The framework describes the components of usability and the relationship between them. According to this approach, in order to specify or measure usability, it is necessary to identify the goals and to decompose effectiveness, efficiency and satisfaction and the components of the context of use into sub-components with measurable and verifiable attributes.

The ISO/IEC 25062 norm provides a standard method for reporting usability test findings. The format is designed for reporting results of formal usability tests in which quantitative measurements were collected, and is particularly appropriate for summative/comparative testing. Stakeholders can use the usability data to help make informed decisions concerning the release of software products or the procurement of such products.

The format includes the following elements: the description of the product; the goals of the test; the test participants; the tasks the users were asked to perform; the experimental design of the test; the method or process by which the test was conducted; the usability measures and data collection methods; and the numerical results.

The Web Accessibility Initiative (WAI), launched in 1996 by the World Wide Web Consortium (W3C), deals specifically with persons with disabilities. While the WAI is not an official standard from the ISO point of view, ISO recognizes the WAI as the primary source of operational guidelines in the field of web accessibility.[56]

WAI refers to the United Nations Convention on the Rights of Persons with Disabilities. It aims at enabling them to perceive, understand, navigate, and interact with systems that contribute to the Web. Web accessibility also benefits others groups such as older people with changing abilities due to aging.[57]

The WAI recommendations are organized according to three different viewpoints:

- Everyone must be able to use the content production tools as well as authorize the production of accessible content. The relevant directives are delineated in the "Authoring Tools Accessibility Guidelines" (ATAG);

[56] Telephone conversation with ISO on March 11, 2012.

[57] See www.w3.org/WAI/intro/accessibility.php [last accessed on 13 November 2011].

- The online content must be accessible. The relevant directives are delineated in the “Web Content Accessibility Guidelines” (WCAG);
- Everyone must be able to use the consultation tools such as web browsers. The relevant directives are delineated in the “User Agent Accessibility Guidelines” (UAAG).

The implementation of WCAG 2.0, issued in June 2010, makes web content accessible to people with disabilities such as blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these.

The Norwegian Approach

The Working Committee

The Norwegian Ministry of local government and regional development appointed in May 2004 a Working Committee to assess the introduction of e-voting in the country. This group published its report, "Electronic voting, challenges and opportunities", in February 2006. The necessity of inclusive elections and of an accessible voting system is explained in the report as follows:

> *“If elections are not inclusive − in terms of the right to vote as well as in terms of being eligible as a candidate – the representativity of the system is weakened. . .If the representation is skewed in relation to the population as a whole, this may in turn skew policy-making and the directions of government action.” (Ministry of Local Government and Regional Development 2006: 43)*

When dealing with the question of the electronic voting pilots, the report stated that:

> *“The main objective of the working committee’s recommendations is to make it easy for voters to exercise their democratic rights and to reduce the costs related to this exercise. To achieve this objective, one strategy is to make e-voting facilities in uncontrolled environments available for all voters. The introduction of an e-voting system will increase accessibility and, in the long run, reduce costs related to running an election, as well as ensuring faster and more accurate vote counting” (Ministry of Local Government and Regional Development 2006: 128)*

This committee therefore saw accessibility as an issue that was not strictly associated with disabilities, but with the broader question of the social representation of the elected representatives. The broader the electorate, the better the representative nature of those elected.

The project mandate

The project mandate for the e-vote 2011-project, published on 1 February 2011, states the following as its main goal: “To establish a secure electronic voting platform for general, county and local elections, providing improved accessibility to voting for all groups (…).” Asking the question “why e-voting?”, the document lists the following reasons for starting the project: increased availability to voters, in particular voters who are today somehow impeded in their voting (e.g. the functionally impaired, expatriates etc.); new generations of voters expect electronic solutions; to provide a quicker and more precise result; to reduce costs in the long term; to enable low cost direct democracy (referendums) (Ministry of Local Government and Regional Development 2011: 5).

The first and second reasons clearly deal with accessibility and usability. Note that increased accessibility is at the top of the list. Details on the requirements for companies tendering in Norway can be found in the document “Accessibility and Usability Requirements part of the tender” (Ministry of Local Government and Regional Development 2009). There, it is requested that the system complies with the WCAG 2.0 AA-level success criteria from WAI, even when using JavaScript. This is the most comprehensive accessibility norm so far.

The Dimensions of Accessibility: an Analysis

Development of the interface

The interface development for the Norwegian Internet voting application started in 2009, when a preliminary study was done on the prototypes of the e-vote client (Fuglerud et al 2009). The Norwegian project group worked in close contact with a reference group and representatives from the different organizations for disabled people and users with disabilities were involved in the testing. With a view to testing and refining the e-voting solution, pre-pilots were conducted throughout autumn 2010 and winter 2010/2011 in the pilot municipalities. In the last two pilots, the solution with return codes was also tested. By May 19, 2011, the 10 pilot municipalities had tested e-voting online either in a youth council election or by arranging local referenda on various issues. Evaluations, consisting of voter surveys and in-depth interviews among the voters and non-voters, were carried out in all the pre-pilots.

In the summer of 2011, a large-scale test-election, open to voters in the pilot municipalities, took place. Delays in the deliveries from a subcontractor prevented a separate user test on the final version of the e-voting client with a sample of disabled people. However, two researchers from the Norwegian Computer Centre did an observation study with 28 disabled people during the advance voting period and this could be a basis for further improvements for the e-voting client.

Looking at other cases of Internet voting, there is no information available on the interface development process for the 2003 and 2006 elections of the Assembly of French Abroad (AFE). In 2009, Extelia, the French company that was Scytl’s partner for that year’s election, organized focus groups together with the AFE to test the interface. These groups were composed of members of the Senate and of the AFE. Only marginal changes were done to the interface after these tests[58].

By contracting an e-voting provider every three years, the French Ministry could only choose between existing solutions, whose provider had little incentive to radically change their product. The time frame allowed did not permit large developments either; in 2009, Scytl was contracted in January and the ballot took place in May. In view of the 2012 parliamentary elections, a test election took place in January 2012 with 20,000 French citizens living abroad who volunteered. An authentication solution was also tested on this occasion.

[58] Phone interview with Jean Souto, head of French projects for Scytl, October 20 2011.

Estonia has not involved average users in the interface development process. However, associations representing visually impaired people were involved in finding the best support for on-screen readers. Public “mock” demo elections are held prior to all actual elections.

In Geneva, tests were conducted with voters and students. In 2002, a PC with the voting interface was installed in the waiting room of the office delivering passports. The public was invited to try the interface. A mock election was also performed with high school students. It must, however, be noted that the trial was a referenda, which does not require as complex an interface as a traditional election. In 2010, an interface was developed for elections. A business analyst developed a first version that was submitted to a two-round review with a specialist of ergonomics and staff from the election department. Finally, a mock election was organized with the mayors and deputy mayors of all 45 Geneva municipalities as well as members of the Geneva parliament as voters.

Vote accessibility from the voter interface point of view is heavily dependent on the electoral rules of the country considered. The Norwegian system is moderately complex, more than the French and the Estonian, but less than the Swiss. Norway has adopted the most formal process of stakeholders’ involvement. It has also a more complicated system, because of the return code (use of two channels to interact with the voter), which was coherent with its overall approach to the project.

The interface development phase offers a good opportunity to allow citizens and politicians to get acquainted with the system and Internet voting. Norway skillfully used this opportunity, while France and Geneva did to a lesser extent. Mock elections are an integral part of this approach. Time is an important parameter for a successful stakeholder involvement. Norway took time, as it started its interface development and testing two years ahead of the election.

Voter Identification Process

The most common way for Norwegian voters to identify themselves to vote online is through the MinID eGovernment portal. In recent years all Norwegian taxpayers received a letter with the PIN codes needed to use MinID, regardless of whether they had requested them. All students finishing school also receive such PIN codes as they leave. Users must activate their MinID account by registering with an official website and creating a password.[59] If users want to make use of the one-time code sent by text message option, they must provide a cell phone number (which is otherwise optional). It was not possible to vote online without registering a cell phone.

MinID relies on a two-step authentication process. When accessing the MinID web page, voters are asked for their social security number and the password they have themselves defined. They then receive the one-time password on their mobile phone, which is used to complete the authentication process. The ID system used for the online state lottery (BuyPass) and Commfides (which issues e-ID certificates) were also available as they are considered as secure as MinID.

[59] The process involves creating a password for MinID, registering an email address and mobile phone number, and choosing whether you want to use one-time access codes sent to your mobile phone of the permanent access codes from the PIN-code letter – see http://minid.difi.no/minid/spm.php?lang=en [last accessed on 20 February, 2012].

The use of MinID to identify voters is coherent with the previous development of eGovernment in Norway. Some 2.6 million people have activated their MinID account out of a total of 3.8 million eligible voters (68 percent).[60] This means that all eligible voters are potential MinID users, but not all have activated their account. Because of the universal distribution of PIN codes, one can assume that all interested Norwegians have activated a MinID account and that as a consequence most potential users of Internet voting actually have the possibility to use it. It is possible to speak of generalized access to Internet voting in Norway among the population that has previously shown an interest in eGovernment. It must be underlined here that it was possible even during the advanced voting period to activate one's MinID account in order to vote.

One could reasonably assume that disabled people have a stronger incentive to request a MinID account, since being able to deal remotely with their administrative affairs would bring them a higher benefit than for non-disabled people. In an article, “Enkelt E-valg?”, Ingvar Tjøstheim and Kristin Skeide Fuglerud report on their study on vote accessibility for voters with disabilities in the municipalities of Re, Sandnes and Ålesund. They write: “We have seen a lot of cases where voters have not understood what to do to be able to vote electronically. Some will need help to register as MinID user. They cannot read PIN codes, or cannot combine passwords and pin codes correctly." Tjøstheim and Fuglerud continue: “The threshold for using e-voting would certainly be lowered if the sign-in solutions were more user friendly and accessible” (Tjøstheim and Fuglerud 2011).[61] This may be linked to the fact that the majority of visually impaired persons in Norway are in the 60+ age group.

Figure 5 below shows that only 16 percent of 190 visually impaired respondents found MinID very easy to use. The age factor is strong, however; 54 percent of the 15-24 year olds find it easy to use MinID, while only eight percent of the 60-75 age group share this statement.

[60] This figure is taken from the Agency for Public Management and Egovernment (Difi) website – see http://www.difi.no/elektronisk-id/about-the-use-of-electronic-id [last accessed on February 12, 2012].

[61] Quotes are translated from the original Norwegian using Google Translate.

Figure 5 – Opinions on Ease of MinID Use (2010)[62]

Age	Not relevant / Don't know	Very difficult 1	2	3	4	5	Very easy 6
15-24	20%	5%	0%	5%	16%	10%	44%
25-39	27%	19%	13 %	1%	8%	27%	6%
40-59	42%	16%	8%	7%	3%	20%	4%
60-75	69%	16%	4%	4%	0%	0%	8%
All (weighted)	57%	16%	5%	4%	2%	6%	10%

Source: (Tjøstheim 2011)

From the accessibility point of view, it is positive that no element on the voting card voters receive at home is needed in the voting procedure;[63] so is the fact that the MinID client warns the voter when a wrong password has been typed in.[64]

In France, for the 2003 election of the AFE, voters received by post from the administration a code and a password enabling them to identify themselves on the voting web site. In 2006, voters who wanted to vote online had to register with the administration, by post or electronic mail, at least six weeks prior to the election. They received three weeks prior to the ballot day, at the latest, the identifiers allowing them to vote online.

In 2009, the French administration tried to leverage the AFE election to attract more expatriates to the GAEL[65] eGovernment platform that is dedicated to them. To this aim, expatriates who wanted to vote online had to create a GAEL ID by logging on the GAEL platform using their consular identification number (NUMIC), their name, birth date and passport Nr and, in a second time, define their own 8-12 alphanumerical characters-long single use password for the voting procedure.

The Estonian Internet voting system builds on the Estonian ID card. This card is a chipped picture ID card using the standard state supported X.509 public key infrastructure. It allows for secure remote authentication and legally binding digital signatures. As of January 2011, more than 1.1 million people (almost 90 percent of the population) had such a card.

To vote, citizens are issued two passcodes to be used with the card. Authentication requires a card reader. These are inexpensive, easy to buy and widely available on computers in public spaces such as public libraries and Internet cafes. In 2007, Estonia introduced a mobile-ID system where a mobile phone can be used as ID card and card reader at the same time. It offers the same functionality in terms of authentication and digital signature as the regular ID.

[62] This is not data from the 2011 survey of voters with disabilities, but from a 2010 study of 190 visually impaired respondents.

[63] Confirmation codes are not needed to cast a ballot.

[64] Whether this facilitation also makes sense from the security point of view is an issue that should not be overplayed. If an internet voting system had a 100%-secure client side, the odds are high that it would not be used because it would be too cumbersome for most voters.

[65] GAEL is the acronym of Guichet d'Administration Electronique.

Geneva decided at the start of the project that Internet voting should be open to all. This is reflected in the authentication process in that no special device, no piece of hardware and no pre-registration are needed to vote online. For each ballot, citizens receive at home a single-use voting card, which carries some of the information they need to vote online. The information that is not reproduced on the card represents “shared secrets”[66], in other words, information known only to the voter and the system.

The voting card contains a unique voter number and a password. Both are changed for every ballot. To identify himself, the voter must type his number into the voting web site, fill his ballot, and type in his password. Then, he must share his secrets with the system, namely his birth date and municipality of origin (the commune where his family acquired its political rights). Birth date and municipality of origin were chosen because they are not public data (no public register contains them).

The e-voting project has shown that some birth dates in the voter register (and hence in the population register) are wrong. Municipalities of origin may also be tricky as some voters have more than one, while the system only knows one for each voter. This open-to-all procedure has one limitation. Resident foreigners, who may vote on communal matters, have no municipality of origin. Their identification for online voting is therefore a bit less secure than for Swiss citizens.

Managing the identification method and procedure in Internet voting is a game of trade-offs between security and accessibility. Norway chose to be intransigent on security. The use of two communication channels clearly raises the barrier to identity theft. On the other hand, the preregistration requested to get a MinID and the request to provide a cell phone number create hurdles that do not exist in Estonia or Geneva.

France chose in 2003 a simple system. Success measured in terms of increased overall turnout, which was the officially stated aim of introducing Internet voting, was, however, not achieved. The lesson here is that electronic voting systems must be developed with the voters and not for them, as was the case that year. In the subsequent elections, the need to preregister added a hurdle whose added value in terms of security is not immediately clear.

Estonia proactively distributed its electronic ID card before introducing Internet voting. This approach, however, requires the voter to have an extra piece of hardware: a card reader. While the X509 norm may be seen as weak in terms of authentication, the move towards mobile ID introduces a second communication channel and a greater security. Yet, less than two percent of voters used mobile ID in the 2011 parliamentary election (OSCE/ODIHR 2011: 11).

The Estonian system is simple and accessible, even for visually impaired people. The level of authentication and security it provides is however lower than in Norway, on at least two counts. The X509 norm is no longer the safest way to handle online identity and the use of a single channel for the voter authentication and the vote is no longer a best practice.

[66] These shared secrets are the date of birth of the voter and the municipality of origin of the voter. While the date of birth may be data which is relatively easy to find, the municipality of origin is data which is not used in other contexts, so would be much more difficult to use fraudulently.

Geneva developed the most open and simplest authentication system of the four. Geneva's initial requirement was that Internet voting should be open to all. Here, the trade-off favors accessibility. In theory, by stealing a voting card, anyone could vote online. This is, however, mitigated by the use of "shared secrets", information likely known only to the voter and the administration. The idea is similar to that of the French request for voters to create their own password, but it uses data already in possession of the administration.

The voting procedure

One of the objectives of the Norwegian system was to comply with the WCAG 2.0 AA-level success criteria from WAI. For the paper-based voting procedure, there were ballots printed in Braille. What about the online procedure from the visually impaired point of view? Tjøstheim and Fuglerud write, "Most participants in our study were able to make a party vote without amendments when they first logged on." Some participants to their study tried e-voting, but did not succeed in casting a vote either because they had not read or understood the instructions, they lacked IT skills or experience, or they were stopped by the message "an error has occurred."

Tjøstheim and Fuglerud underline that being able to cast several votes is valued by visually impaired voters: "Many of the participants felt that this (…) gives them greater confidence and control than with paper-based elections." However, they also mention that several participants had trouble finding out how to give personal votes. They suggest that this was due to a lack of knowledge about the personal vote as well as to deficiencies in the design of the user interface and conclude that a greater focus on universal design will allow more visually impaired people to be self-reliant and independent as they vote (Tjøstheim and Fuglerud 2011).

The helpdesk did not register calls regarding the possibility to cast personal votes (see the table below in the "helpdesk" section). We may conclude that the add-on process was simple for non-visually impaired voters. A positive feature was the possibility to vote for the two races (local and regional) at different times, or to revote only online for one of the two races. The voting web site was also available in seven languages: Norwegian Bokmål, Norwegian Nynorsk, English, Polish, Russian, Somali, and Serbian/Bosnian/Croatian.

In France the W3C norms were not considered in any of the three elections to-date for the AFE. Neither the 2003, nor the 2006 and 2009 systems complied with it, as it was not part of the French government requirements. For the 2012 parliamentary election for French abroad, the state has added compliance with W3C norms to its requests. In 2009, Scytl, the service provider to the French state, worked to reduce the size of the Java applet that its system uses to allow voters in South America and Africa to vote using dial up Internet connections. The web site had been developed in French and English, but only the French version was used, as the Ministry could not justify the use of a foreign language on an official web site.

In Estonia, IFES was informed that the system is fully W3C compliant, but no further details were provided. The web site dedicated to the project offers no information on this issue. In 2008, when refurbishing its Internet voting application, Estonia had to choose between a standalone downloadable application and a "Java" based solution running within the web-browser. While the latter is more convenient to use, the former is considered more secure. The choice was made to develop the downloadable standalone solution.

Regarding languages, the voting web site is only available in Estonian, which is the official language of the country. The OSCE has regularly questioned the issue and suggested that Russian should also be offered. Although no statistic is available, the Estonian project manager indicated that a considerable number of voters started a voting session without finishing it. This may reflect voter's curiosity, the desire to try out the solution before voting for good at a later stage, or real trouble with the application. This issue deserves more investigation.

The Geneva voting web site is largely but not totally compliant with the WCAG norms. A new release in the first half-year of 2012 should be compliant with the AA level of the WCAG norms. To achieve this compliance, a few "comfort" functions, programmed with Javascript, will be suppressed. This is for example the case of the automatic self-positioning of the cursor in the fields to be filled.

Currently, the difficulty for disabled voters are related to the use of Javascript fields and to the lack of labels for the fields to be filled, such as the birth date field for voter authentication or the unfolding list of municipalities, where the voter has to choose his commune of origin in a list of 50. The voting card also poses a problem to visually impaired voters. The password to be inserted into the voting web site is hidden behind a hologram to be rubbed off. This is not done to protect the voter against vote theft, but to allow polling station workers to see who might already have voted online.

Geneva does not provide a hyperlink to its voting web site for security reasons: redirecting the voters towards the voting site entails the risk of a man-in-the middle attack, where voters are pointed towards a counterfeit voting web site. Voters must thus type the full address https://www.evote-ch.ch/ge to start a voting session. Every second voter forgets the "S" in "https." This choice has been repeatedly criticized by the media, where it has been called absurd from the usability point of view.

As Switzerland has four official languages (German, French, Italian and Rumantsch), it is a legal requirement to provide all of them for federal ballots. The website is therefore offered in these four languages. The site also contains integrated tools to help voters. A clickable image of the voting card indicates where to look for the password or the site's certificate's fingerprint. A link opens a new window with the FAQs, the official explanatory brochure for referendums and to the political parties' vote recommendations. For elections, moving the mouse over the candidates' name displays a floating window with the information that the political parties otherwise print on the ballot papers, usually the age, commune of residence and profession of the candidates. An analysis of the logs for the November 27, 2011, ballot shows that some 240 voters started a voting session without finishing it. As there were 15,791 ballots cast online, the unfinished sessions represent 1.5 percent of the online cast votes, which is a low figure.

The Return Code

The return code is meant to build widespread trust by offering a level of transparency previously unknown in remote electronic voting. It also ensures a high level of usability, providing the lesson from the Dutch Internet voting system, RIES, is learnt (Pieters 2006). Before RIES was actually used in an election, trial sessions revealed that a difficult verification procedure decreases trust in the system. In Norway, the return code has been simplified in the sense that it does not give full information about any personal votes on the ballot. To do so would have resulted in a complex return code for the voter. As it is important from a security perspective that the message is read and understood, it was decided not to include this information in the return code.

Voters who have not registered a phone number with their MinID could not use Internet voting, as the return code feature requires this mobile phone number. It could be considered that not recording a mobile phone number with the administration is a personal choice of the citizens and must not be considered as an accessibility issue. As far as visually impaired voters are concerned, for the September 2011 pilot, neither was the voting card printed in Braille, nor was it formatted for devices reading out loud written text. The only facilitation was the use of large, black fonts on yellow paper. Visually impaired voters could verify their return code either by using a magnifying lens or by asking someone to check for them whether the code they received matched their choices according to their voting card.

In their study conducted in the municipalities of Re, Sandnes and Ålesund, Tjøstheim and Skeide, Fuglerud write that checking the return codes "is more complicated for the visually impaired people than for most other voters" (Tjøstheim and Fuglerud 2011). The Ministry of Local Government and Regional Development recognizes there is room for improvement in the design of the voting card to help visually impaired voters performing this check. We do not discuss here the use of cell phones as there are devices to allow visually impaired people reading their text messages.[67]

An unknown number of voters received a return code that did not match the one on their voting card corresponding to the party they had voted for. One hundred nine voters called the helpdesk, which brought the issue to the fore. Incorrect codes were printed on their cards, probably as a result of a mistake in the generation of the printer's files. This usability issue calls for a review of the procedures for this printing process.

The management and organizational challenge posed by the codes is also illustrated by the 26 further calls received by the helpdesk regarding the codes. Eleven voters had not received a voting card and could not check the codes, five voted online but did not receive a code, four had no codes printed on their voting card, three had questions on how to use the code, and one received two voting cards with different codes. The two voters who received return codes while not having voted online may, on the contrary, be proof of the validity of the code concept.

France had no return code in 2003 and 2006. In 2009, voters received the standard Scytl return code, confirming that the vote had reached the ballot box. There is no return code in the Estonian Internet voting system. There is also no return code in Geneva. As with the Scytl system, voters get a message on their PC confirming that their vote has been stored in the ballot box at a given hour on a given day. It is possible to call this message back anytime by again inserting the voting card number in the voting web site.

[67] See for example www.visionaustralia.org.au/info.aspx?page=1502 [last accessed on November 16, 2011].

The return code is a leap forward in Internet voting. It is one of the features distinguishing second-generation Internet voting systems from first generation ones, such as the one in Geneva. The Norwegian system implements verifiability for all three components of the process - cast as intended, recorded as cast and counted as recorded. However, individual verification is only possible for the first of these components – cast as intended. The zero-knowledge proofs provide E2E verifiability on a system level for all three components. In this context, an increased level of individual verification is not a must for the system, but a feature which would be nice to have.

The Voting Period

In Norway Internet voting was offered as a supplementary method of advance voting. It was possible to vote online from August 10 - September 9 at 23:59. It was also possible to vote on paper from July 1 - September 9 in any municipality; any voter could cast a ballot for his municipality by going to any advance polling station in Norway and the vote would be transferred to the correct municipality. The deadline for voting on paper abroad was September 2.

France changed the duration of advance voting for each of its three online elections. In 2003, there were 13 days to vote online. Internet voting ended the day before the polling stations opened. In 2006, there were seven days to vote online. Internet voting ended 5 days (a working week) before the polling stations opened. In 2009 there were 15 days to vote online. Internet voting ended two days before the polling stations opened.

Estonia initially offered Internet voting during three days, from the sixth to the fourth day before the polling stations open. In 2011, this period has been increased to seven days, from the tenth to the fourth day before the polling stations open. From the thirteenth to the ninth days before the election, voters can also cast an early paper ballot in one of the advance voting polling places. There is one such location in every municipality. In the sixth to the fourth days, a voter can vote by paper ballot at a larger number of polling places.

In Geneva, the advance voting period starts 28 days before the polling stations open and closes 22 hours before their opening. This does not mean, however, that the voters have received their voting card 28 days before the polling days; it is, rather, a standard operation window for the Internet voting. The law prescribes that the voters must receive their voting material three weeks before polling days for federal ballots and 10 days for cantonal and municipal ballots.

While an extended voting period increases accessibility, the discussions in the focus group conducted by IFES in the framework of the study of the efficiency of counting showed that some voters expected to vote online on the polling station opening day, September 12, as this was the day identified with the election.[68] In Radøy, one of the respondents stated that “most young people always are acting at the last minute. Internet voting was closed on Friday, and many believed that they could vote online on the weekend as well.”

[68] See for instance the in-depth interview in the municipality of Radøy or the discussion within the focus group 1.

In other instances of Internet voting, there has been a clear trend towards late voting, that is casting a ballot towards the end of the Internet voting period. In their study, “Internet Voting in Estonia: A Comparative Analysis of Four Elections since 2005”, Trechsel and Vassil observe that “in both elections in 2009 the number of e-voters started to grow after the third day of early voting” (Trechsel and Vassil 2010: 23).[69] They point to the “importance of the length of the voting period as an important determinant of voting activity, especially if considering e-voting as a means of convenience voting” (Trechsel and Vassil 2010: 23-4). In Geneva too, many Internet votes are cast during the last 36 hours of the Internet voting period.

Supported Client Configurations

Ten years ago, when Geneva stared its e-voting project, the number of browser/operating system combinations was smaller than today and the market more compact. Windows’ share of the market was 98 percent and Internet Explorer’s 80 to 85 percent. Today, while Windows is still the dominant operating system, Internet Explorer’s share had fallen significantly with many other browsers now being used.[70] This situation is a challenge for developers; the more so as Java, which also has different versions, is often used in secure applications. Furthermore, the timing of the release of new operating systems, browsers or Java versions is in the hands of the software producers. The longer the advance voting period, the higher the probability that at some point a new release taking place during a voting period, hindering the usability of the voting site. Since 2003, this has happened at least three times in Geneva. Voters had to install a second browser to resolve this issue.

In the Norwegian case, data from Finn.no, Norway’s largest online market place (labs.finn.no), was used to determine the browser/OS combinations that should be supported for the Internet voting system. In addition to this feedback was received from national reference groups (such as the Norwegian Association of the Blind and Partially Sighted, and the Norwegian Labour and Welfare Administration), which provided information on browser/OS configurations that people with disabilities were using.[71] The resulting list of supported configurations is shown below in figure 6.

In France in 2009, all standard combinations of the most common browsers with Windows, Mac OS and Linux were supported. The Estonian Internet voting application supports Windows XP SP 3, Windows Vista and Windows 7, Linux (Debian 5.0, openSUSE 11.3, Ubuntu 10, Fedora 14) and Mac OS X 10.4 Tiger, 10.5 Leopard, 10.6 Snow Leopard, combined with the most common browsers. The choice of supported configurations was made based on the most commonly used platforms in the county.

In Geneva too, the choice of supported configurations is based in the most common configurations used by the visitors of the state web site. The supported configurations cover 90 to 95 percent of the web site visitors’ systems. The Geneva systems supports Windows 2000, XP, Vista and Seven combined with a recent release of IE, Firefox, Chrome, Safari or Opera. For Mac OS X, the supported browsers are a

[69] The advance voting period had been extended from 3 days to 7 days in 2009.

[70] In October 2011 Internet Explorer’s share stood at 52.6%, Firefox at 22.5%, Chrome at 17.6%, Safari at 5.4% and Opera at 1.6%. Source www.netmarketshare.com/ [last accessed on November 20, 2011].

[71] Email from the Ministry on February 9, 2012.

recent release of Safari, Firefox, Chrome or Opera. For Linux (combined with Java Sun, Linux Java is unsupported), it takes a recent release of Firefox or Chrome to vote online.

The simple landscape of the early 2000s will not come back, even if a new wave of consolidation among browsers may happen. The issue of compatibility will remain and will continue to cause headaches to developers. As browsers are free and simple to download, one solution could be to push e-vote users towards a limited number of browsers, but this is likely to cause discontent among voters. A solution could be to create a voting client independent from the browser.

Figure 6 – Operating System/Browser Configurations Supported by the Norwegian Internet Voting System

Browser/OS	Win XP	Win Vista (32)	Win Vista (64)	Win7.0 (32)	Win 7.0 (64)	Linux (32)	Linux (64)	OS X (10.5)	OS X (10.6)
Java	1.6	1.6	1.6	1.6	1.6	1.6	<1.5>	1.6	1.6
IE 6	**[x]**		**x**			not exist	not exist	not exist	not exist
IE 7	X	x	**[x]**			not exist	not exist	not exist	not exist
IE 7 (64)	not exist	BL	BL	not exist		not exist	not exist	not exist	not exist
IE 8	X	**[x]**	**[x]**	x	**[x]**	not exist	not exist	not exist	not exist
IE 8 (64)	not exist	not exist	BL	not exist	BL	not exist	not exist	not exist	not exist
IE 9	not exist	**[x]**	**[x]**	x	**[x]**	not exist	not exist	not exist	not exist
IE 9 (64)	not exist	not exist	BL	not exist	BL	not exist	not exist	not exist	not exist
FF 3.5	X	x	**[x]**	x	**[x]**	x	**[x]**	BL	**BL**
FF 3.6	X	x	**[x]**	x	**[x]**	x	**[x]**	BL	x
FF 4.0	X	x	**[x]**	x	**[x]**	x	**[x]**	x	x
Opera 10.6	X	x	**[x]**	x	**[x]**	BL	BL	x	x
Opera 11	X	x	**[x]**	x	**[x]**	BL	BL	x	x
Safari 4.5	BL	BL	BL	BL	BL	not exist	not exist	BL	BL
Safari 5	X	x	**[x]**	x	**[x]**	not exist	not exist	x	x
Chrome	X	x	**[x]**	x	**[x]**	BL	BL	x	x

Legend: x = supported; [x] = limited support; BL = Black Listed; <1.5> = Java 1.5 not supported, only Java 1.6 is supported.
Source: Ministry of Local Government and Regional Development - Matrix final v2.7 - 02.05.2011

Helpdesk

In Norway 698 calls were received by the helpdesk with 641 enquiries being answered.[72] Compared to the 27,554 Internet votes recorded for the municipal election, this represents one call for each 39 votes (2.5 percent). This low figure, especially for a first-time use, testifies to the application's ease of use. Two issues stand out among the calls received by the helpdesk: problems with Java (235 calls or 45.2

[72] Data provided by the Ministry in email of November 2, 2012.

percent of the total) and with the return codes (109 calls for wrong return code, or 21 percent of the total, 135 calls altogether regarding the codes, or 26 percent of the total). The third motive of calls to the helpdesk, problems with the login procedure, is an order of magnitude behind the first two: 47 calls, or 9 percent of the total.

The in-depth interviews conducted by IFES in the pilot municipalities confirmed the problems with Java. The large share of calls regarding Java indicates that its integration in secure web applications is problematic. The very large number of supported configuration may explain the Java share in the calls to the helpdesk. The return code and MinID have been dealt with in the relevant sections. While the former is more an organizational issue, linked to the complexity of handling correctly voters' lists compiled at the municipal level, and then completed with personal return codes generated at the central administration level, the latter is a real accessibility issue.

In France in 2009, the helpdesk was managed at the embassy level and no consolidation of the queries has been done. It is impossible to have detailed data on the difficulties voters have encountered. There is also no data on the 2003 and 2006 operations.

During the March 2011 Estonian parliamentary election, the helpline (both phone and e-mail) received a total of 1,418 contacts, which represents one percent of the total number of Internet voters. The main issues raised were the setup and use of the ID card, connection problems with the voting client and problems linked to the setup of the Mobile ID solution. This was the fourth online election in Estonia. Although the application had changed (new voting client to be downloaded), the number of requests to the helpdesk was very low. This must, however, be mitigated by the quite large number of voters who started a voting session but did not finish it.

In Geneva, the number of requests introduced to the helpdesk has decreased in 2011[73], following work on the application aimed at improving its compatibility with the various OS/browser configurations and allowing the voting procedure to transit through other ports than port 443 of the voters' PC.[74] Many citizens vote from their working place and network restrictions were deeply resented. They were the cause of up to a quarter of the calls to the helpdesk.

Number of Voting Channels

The accessibility of voting is definitely enhanced by offering a remote voting channel, such as Internet voting. Yet not everybody trusts Internet voting, not everybody has a PC or makes online transactions and, in the French or Norwegian case, not all citizens pre-register to have or use their online ID. In this context, providing a paper-based remote channel, postal voting, is not duplicating Internet voting, but rather complementing it.

Of the cases surveyed here, France, Geneva and Norway offer postal voting as well as Internet voting and voting in polling stations. Estonia only offers Internet voting and voting in polling stations.

[73] Decreased from 2.1% of internet voters in February 2010 to 1.3% of internet voters in November 2011.

[74] Port 443 is oftenten blocked on companies' IT networks.

Conclusion

The Norwegian Internet voting application has reached a very high degree of accessibility, especially given the fact that the September 2011 ballot was its first use in binding political elections. Improvements can be made, however, to help visually impaired voters cast a vote and check the return code without external help. It remains also to be seen whether target groups such as young voters and expatriates made use of online voting. This is also an accessibility issue.

The Role of Stakeholders

Internet voting changes conventional electoral patterns in many ways and one of them relates to the different roles that relevant stakeholders have to adopt. Not only do new stakeholders assume prominence in the Internet voting process, such as voting technology suppliers, but existing stakeholders have to adapt their roles in order to fulfill their existing functions. This new network of stakeholder roles and relationships may be difficult to manage, with some of the demands of stakeholders being contradictory (for example, different positions on disclosure of information on Internet voting systems) (Hall 2007: 3-5, Barrat-Esteve 2010).

Central to this new network of stakeholder relationships is public administration, and especially the EMB. Public administration, and the EMB, will establish the legal and regulatory framework for implementation of Internet voting, and this framework will define the roles and rights of the various stakeholders in the Internet voting process. The EMB will also need to manage the implementation of Internet voting technology, ensuring that they maintain control over the supplier and facilitate open involvement of all relevant stakeholders in this implementation (Goldsmith 2011: 30 and 41-42). As outlined in the thematic section on transparency and trust, an open information policy will be essential to the EMB's interactions with stakeholders in this respect if it is to develop trusted relations with these stakeholders while implementing Internet voting.

Election management bodies need to be especially sensitive and responsive to opposition and concerns about the introduction and use of Internet voting systems. While there will likely always be some that will oppose such systems, ignoring such opposition and concerns is risky. Even small groups opposing voting technology can have a significant impact by raising concerns which resonate with the public.[75] EMBs that fail to respond to concerns about Internet voting may lose control of any public debate in Internet voting in a way that could be fatal for Internet voting implementation. Proactive engagement with opponents of Internet voting by the EMB and attempts to mitigate these concerns will serve to diffuse potentially damaging public debates on Internet voting. It will also help ensure that Internet voting does not become a key, or divisive, issue in the country's political discourse.

Stakeholder Surveys on Internet Voting

Public opinion of Internet voting is difficult to measure without opinion surveys, and unfortunately these surveys are relatively sparse. Fluctuations in turnout, or the percentage of votes cast via the Internet, are unreliable metrics of public perceptions. It is difficult to measure, for example, if Internet voters are

[75] See the later section on examples of discontinued electronic voting experiences, and especially the examples of Ireland and the Netherlands where civil society was very effective in rallying support against the use of electronic voting machines.

new voters, or previously engaged voters who are trying a new method of casting a ballot. The ability to conduct surveys is often made difficult given the small size of Internet voting pilots. In the United States, for example, the West Virginia Internet voting pilot was extended to only eight counties, resulting in a total of 125 Internet voters (Tennant 2011: 3). Furthermore, as many Internet voting projects (e.g., France and the United States) are limited to expatriates, widespread knowledge of the system may not exist among the general voting population.

Surveys that have been conducted, however, demonstrate a general acceptance of Internet voting among those who have used it. In the town of Markham, Canada, a large majority (78 percent) of online voters described themselves as “very satisfied” with their experience in the 2006 municipal election. Furthermore, 91 percent stated that they would be ‘very likely’ to vote online in the future, while 80 percent said they would be ‘very likely’ to recommend online voting to others. In a separate question, 90 percent said they would be ‘very likely’ to vote online in a provincial election if the option was offered, with that number being 89 percent for federal elections (Delvinia Interactive 2012: 3-4).

Similarly, a report conducted to evaluate satisfaction with the New South Wales (NSW) State General Election in 2011 showed a high level of trust in the system. The vast majority (96 percent) of Internet voters were either very satisfied (86 percent) or somewhat satisfied (10 percent) with their experience (Allen Consulting Group 2011). In Switzerland, 98 percent of Swiss nationals from Bern who voted from abroad in the May 15, 2011 election stated they would vote via the Internet in the future, indicating strong satisfaction with the system.[76] It could be argued, however, that in these surveys, self-selection bias is leading to an inflated perception of Internet voting. In other words, those who do not have confidence in Internet voting are not likely to cast an online ballot in the first place.

These same polls indicate that those who choose to cast an Internet ballot generally do so for convenience. Eighty-eight percent of online votes in the 2006 Markham election cited this as the reason they voted online; a number similar to those who voted in 2003. This claim is supported by the fact that roughly 20 percent of those aged 18 - 34 cited being “out of town during the election” as the reason for voting via the Internet (Delvinia Interactive 2007). In New South Wales, respondents also generally felt that the main benefit of Internet voting was the convenience it offered them. As the New South Wales program was targeted at voters with disabilities, most respondents indicated that Internet voting made it far easier to cast a ballot. This included not needing to make a trip to the polling station, and having an easier time casting a ballot in general (Allen Consulting Group 2011). The reasons for voting online are similar in Estonia, where an average of 75 percent of those who cast an Internet ballot across four elections listed convenience as the reason for their decision (Trechsel and Vassil 2010).

Public trust in Internet voting has been mixed depending on the local context. Increased confidence in Estonia’s system can be verified, not just in increased usage, but in trend data from public opinion surveys. Not only has skepticism of the project decreased, but confidence among Internet voters has intensified. Furthermore, when non-Internet voters have been asked the reason for casting a traditional ballot, security concerns were rarely mentioned. Instead, most voters gave reasons related to not having

[76] www.be.ch/portal/fr/index/mediencenter/medienmitteilungen/suche.meldungNeu.html/portal/fr/meldungen/archiv/archiv9/mm_9798 [last accessed January 16 2012].

either a computer or Internet access (Trechsel and Vassil 2010). Similarly, in New South Wales, only three percent of those who were eligible to cast an Internet vote but did not, mentioned that it was due to concerns over the technology (Allen Consulting Group 2011).

Although trust in Internet voting can be high, it is vulnerable to public accusations of political and demographic bias. Politics cannot be removed from electoral operations, no matter how technical in nature. Even extending the franchise is not without controversy as certain stakeholders can be expected to benefit more than others. The supervised Internet voting pilot in Okaloosa County, Florida, for example, was perceived as benefitting Republicans, due to the fact that the target voting group (U.S. military personal overseas) was more likely to be Republican.[77] In Switzerland, Internet voting is opposed by the Geneva Green Party, who do not trust the system, and the nationalist Union Démocratique du Centre, who are against remote voting in general. In Estonia, the Centre Party is thought to be under-represented among Internet voters, while the Pro Patria Union is over-represented.

The concept that Internet voting may be used more by different segments of the population is not without merit. Studies have provided strong evidence that both age and income have a significant impact on inclination to use Internet voting (Belanger and Carter 2010). There have been some exceptions to this trend, however, as survey data from Canada indicated that those over 55 were the most likely to try Internet voting (Delvinia Interactive 2007). Furthermore, while Estonia's history with Internet voting mostly conformed to the notion that younger voters were more likely to use the system, the 2009 election witnessed nearly equal participation rates up until the age group of 40-49. This still reveals that younger voters are more likely to become early adapters of the technology, and more than likely, place a higher level of trust in the system initially (Trechsel and Vasill 2010).

Despite these concerns, however, there is mixed evidence of Internet voting's potential to actually mobilize new voters. Very few seem to view the convenience offered by Internet voting as a reason to vote by itself. This indicates that most potential voters do not view Internet voting as a significant reduction in the marginal cost of political participation. Trechsel and Vassil did find some evidence that Internet voting could increase willingness to turn out among some inconsistent voters. This effect became weaker, however, as political participation of the individual decreases (Trechsel and Vassil) 2010). Other studies of Estonia, however, have indicated that Internet voting merely acts as a substitution for those who would have cast a ballot anyway (Bochsler 2010). The Markham Town report, despite claiming that Internet voting "levels the playing field, giving everyone equal opportunity to engage in the electoral process," acknowledges that their typical Internet voter was already politically active (Delvinia Interactive 2007).

Summary of Global Experiences

The countries which have been found to be comparable in Internet voting around the world vary widely in scope and functionality. Early cases of Internet voting were certainly less advanced technically than those being developed more recently, and many of these changes have been aimed at improving the

[77] Interview with Paul A. Lux, Supervisor of Elections, Okaloosa County, Florida, July 2011.

quality of election delivered by the Internet voting system and meeting emerging standards for electronic voting.

It is fair to say that Internet voting is not a commonly used means of voting, with only 11 countries having so far used it in any form, and only seven of these 11 countries currently having any intention of using it in the future.[78] However, this low level of usage globally needs to be put into the context of Internet voting being a relatively new voting technology, and one that has been developing significantly over the previous 10 years. Internet voting seems to fit, for many countries, a niche corner of the electoral system, largely targeted at those who cannot attend their polling station in person on Election Day.

In fact, many more countries have expressed or shown an interest in the use of Internet voting, especially when they have large numbers of expatriate voters – although Estonia and Norway show that it is not only travelling voters who are interested in using Internet voting. Implementation of Internet voting, if it is to be according to emerging standards, is a very technical exercise. It can also pose some difficult political questions if the aim is to facilitate the inclusion of large numbers of expatriate citizens in the political process.

The technicalities of implementing Internet voting systems are largely a result of attempts to reconcile the use of Internet voting with many emerging and existing standards of which elections, in general, and electronic elections, in particular, are required to comply with. These standards include the need for secure online voter authentication, protection of the secrecy of the vote, appropriate transparency mechanisms, testing and certification regimes, etc. In fact, the need for secure online voter authentication mechanisms may be one of the biggest hurdles to the implementation of Internet voting, and would present a challenge for many established democracies (which often do not have an ID card system with secure online authentication mechanisms).

Given the developments in Internet voting systems over the past 10 years and the fact that Norway has joined this Internet voting group only recently, it is not surprising that the Norwegian Internet voting system is one of the more advanced Internet voting systems. In fact, the Norwegian system seems to have adopted many of the better features of other Internet voting systems as well as developing some new functionality and features, which means that it can be seen as setting the standard for Internet voting systems going forward. This is not to say that the Norwegian Internet voting system meets all of the specific challenges related to the use of Internet voting (which will be elaborated later in this report); however, it could be considered to be the best current example of attempting to do so. It is highly likely that the Norwegian Internet voting system will be seen as a standard that other systems will try to emulate in the future.

[78] It should be noted that a number of other countries have stated an intention to use it or investigate its possible use of internet voting.

Internet Voting Case Studies

This chapter of the report will present the results of three in-depth case studies in Internet voting – Estonia, France and Switzerland – Geneva. These examples have been chosen because they represent three of the most widespread uses of Internet voting, not just in the scope (number of voters who are offered Internet voting opportunities) but also in the length of time that these countries have been offering Internet voting as an option to voters. All three examples are also from Europe, and it is expected that these examples will be of interest to Norway as it considers the future use of Internet voting in light of its recent pilots. Each of the case studies goes into much greater detail concerning the implementation of Internet voting in the country than is possible in the previous overview of global Internet voting experiences.

Each of the three in-depth case studies tries to follow a similar structure to that used in the general overview of global Internet voting experiences. Accordingly, each case study provides an overview of the use of Internet voting in the country, before looking at the thematic issues of trust in Internet voting, secrecy and freedom of the vote, the accessibility of Internet voting and the role of stakeholders. It should be noted however that the structure of each case study does vary a bit, and this is indicative of the particular background and features of these three very different examples of Internet voting.

The full case studies are included in the annexes of the report and a comparison and analysis of the three case studies is presented here.

General Comparison of Case Studies

As indicated in the general overview of Internet voting around the world, countries have adopted Internet voting for a variety of reasons and this has had an impact on the way in which each country using Internet voting implements it. This is very evident from the three in depth case studies presented in the annex of the report.

In France there is a strong political imperative to enfranchise the overseas electorate for the 155-member consultative Assembly of French Citizens Living Abroad (AFE, *Assemblée des Français de l'étranger*). Internet voting is only offered for this election, for which the electorate consists entirely of overseas French citizens, and is seen as a way of encouraging participation. In Estonia the provision of Internet voting is seen as a natural extension of a more general provision of government services online, and as such is offered to all voters. The use of Internet voting in Estonia is also greatly facilitated by high levels of access to the Internet amongst its citizens and secure means of online identification – the Estonian national ID card. In Switzerland-Geneva, the general acceptance and use of postal voting made Internet voting a natural extension of existing remote voting mechanisms. In the context of falling voter turnout and the regular consultation with Swiss citizens through referenda, Internet voting was also seen as a logical mechanism to try and sustain participation in these numerous polls.

These backgrounds inform and drive the way in which Internet voting is implemented in each country. The Estonian building-up of e-government is instrumental in the presence of a national ID card with secure online identification mechanisms. Both the Estonian and Genevan systems are based on the widespread penetration of the Internet and, in the Estonian case especially, the confidence with which citizens use the Internet to access other government services. This context is very different for the French AFE, where the principle motivations are accessibility and participation.

These circumstances are evident in the ways in which the different systems authenticate voters. The Estonian use of the national ID card provides a very secure means of authentication for the voters to digitally sign their votes. The Genevan system combines different sources of information (the voting card and shared secrets) to provide a reasonable level of security in authenticating voters. The French system could be seen as the least secure in terms of voter authentication, with online registration for Internet voting. While this online registration requires information that is personal to the voter and may be difficult, but not impossible, for others to discover. However, the French system's prime motivation is encouraging the participation of expatriate voters and it is understandable that under such circumstances the balance between security and ease of access may be found in favor of accessibility.

Trust in Internet Voting

All three Internet voting case studies employ measures to test their voting systems prior to the election, and audit the operation of the systems and results generated by the systems. In all cases, at least some of the entities that are testing and auditing are independent. In the French case, the results of the assessment by the independent expert - authorized to audit source code, cryptography and system architecture - is not made public. Some of the Estonian reports are also not made public (OSCE/ODIHR 2011: 10).

Geneva employs the most trust and integrity mechanisms. In addition to system testing, a separate electoral constituency is created which, on election day, is voted for by the permanent electoral commission as a check that the system is working correctly. Geneva also allows any citizen to view the source code for the Internet voting application, although none have chosen to do so to-date. Once the results are calculated they are also subjected to a series of forensic statistical checks to determine if there is any indication that they might have been manipulated. Finally, the Genevan system is also subjected to periodic audits.

None of the three case studies implement any form of E2E verification mechanisms.

Secrecy and Freedom of the Vote

Measures are taken in all three case study countries to protect the secrecy of the vote in terms of making it difficult to link the identity of the voter to stored vote values, and this is done through encryption mechanisms by the use of 'double envelopes' for the data. Mechanisms are used to protect the data in transit between the user interface and the vote server, through the use of secure protocols for data exchange. Geneva and France also ensure that votes in the ballot boxes are mixed before they are decrypted.

Estonia is the only one of the case studies where specific measures are taken to protect the freedom of the vote, and to mitigate the challenge of vote coercers and vote buyers. These measures take the form of multiple voting for Internet voters, whereby voters can cast repeated Internet votes and only the last one is counted. Estonian Internet voters can also cast a paper ballot in the advance period of voting and this paper ballot takes precedence over any Internet votes cast. Estonian Internet voters cannot, however, cast a paper ballot on election-day, as the names of voters casting an Internet ballot during the advance voting period are marked as having voted on the electoral roll.

The Accessibility of Internet Voting

Of the three case study countries, Geneva has possibly made the most effort to implement an Internet voting platform which achieves high levels of accessibility for as many voters as possible. This has been achieved through ensuring the compatibility of the voting platform with a wide range of operating systems and web browsers and also through ensuring compliance with accessibility standards. While the Genevan system is not fully compliant with WCAG standards, a new release of the system software in 2012 is hoping to achieve AA compliance with WCAG.

The Estonian and French systems have both ran tests with user groups in one format or another to assess the usability of the systems. Estonia also runs mock elections before actual elections to allow voters to familiarize themselves with the system.

Two additional accessibility issues are worth mentioning with respect to the Estonian system. The first concerns the need to use the national ID card in order to vote, which could be seen as a limitation on the accessibility of the Internet voting system. The national ID card is provided to all Estonian citizens and by 2011 almost 90 percent of the population was in possession of the card. Additionally, in order to use the national ID card to authenticate the voter (or for any other online service using the ID card) a card reader is required to be connected to the computer. Not only are these card readers readily available in the Estonian marketplace, but they are also available on computers in many public places, such as libraries. Therefore the need to use an ID card entails little practical restriction on the accessibility of the Internet voting system.

The second accessibility issue related to the Estonian Internet voting system relates to the languages in which it is available, and the fact that it is not available in Russian. Russian is not recognized as an official language in Estonia, despite there being a significant Russian ethnic minority living there, and the failure to provide the Internet voting system in Russian makes it inaccessible to a large number of voters. Evidence of this can be seen from the much lower use of the Internet voting channel, compared to the paper voting channel, by ethnic Russian voters in Estonia (Trechsel and Vassil 2010: 46).

The Role of Stakeholders

One point of similarity between the case studies is the lack of significant stakeholder opposition to Internet voting in all three countries. This is not to say that all stakeholders support the use of Internet voting in these countries, but the numbers of stakeholders actively advocating against Internet voting is relatively small and has failed so far to generate significant public support.

In Estonia, the National Election Commission regularly held briefings on the Internet voting system but these were not attended by political parties until 2011 (OSCE/ODIHR 2007: 19). Furthermore, no significant NGOs have been created in Estonia to conduct the oversight tasks that other associations carry out in France, Belgium or in the U.S.. In Geneva, political parties were initially very cautious about the use of Internet voting, but now only two smaller parties oppose Internet voting.

In France, political parties are allowed to appoint a representative to observe the Internet voting process. Although they did in 2006, they failed to do so in 2009. To some extent this was likely the result of the 2006 observation process where the three representatives appointed all concluded that proper observation of the process was impossible (Pellegrini 2006, Lang 2006, Appel 2006). France does have an NGO which advocates against the use of electronic voting (called *Ordinateurs de vote - OdV)*, but this has focused more on the use of electronic voting machines rather than against Internet voting. Maybe because Internet voting has been used exclusively to date for French elections to the expatriate representative body the issue has not generated much domestic stakeholder reaction. Greater attention may be paid to Internet voting by French domestic stakeholders in 2012 when Internet voting will be used for the direct election of seven expatriate representatives in the French parliament.

4. Electronic Voting Experiences

Voting technology has been in existence for a surprisingly long time, with the first mechanical voting machines being introduced in the U.S. in 1892 as a means to mitigate the manipulation of cast ballots during the counting process. Punch card voting and counting, which appeared in the U.S. in the 1960s, and mechanical voting machines were still very popular in the U.S. until 2000 when they accounted for the system offered to nearly 48 percent of voters.[79] The first use of electronic voting machines was in the U.S. in 1975, in the counties of Streamwood and Woodstock, Illinois (Jones 2003). It was not until the 1990s that the use of electronic voting machines became more widespread, and countries such as Belgium, Brazil, India and the Netherlands started to implement them in increasing numbers.

This section of the assessment will provide a brief overview of global experiences with non-remote electronic voting machines. Again, it is worth noting the kinds of experiences that this section will and will not review. As discussed in the introduction, a definition was agreed upon by the assessment team to determine which cases of both Internet voting and electronic voting would be covered by the assessment. According to this definition, cases would be included where voting technology was used to hold a “binding vote (elections or referenda) of a political nature.”

This definition excludes cases where electronic voting machines have been used for mock or test elections only - there are a number of countries that have only experimented with electronic voting on this basis. It also excludes a large number of countries which are currently at various stages of considering the use of electronic voting technology, but have not yet used it to conduct a binding vote of a political nature.[80]

In this overview of global experiences of electronic voting, we will first look at the events of the 2000 U.S. presidential election, which represented in many ways a defining moment in the development and perceptions of voting and counting technologies. Then we will provide a statistical overview of how many countries are using or experimenting with electronic voting and at what stage these countries are in their use of electronic voting. Any regional and global trends will also be discussed. A review will be provided of the general kinds of benefits and challenges that are offered by using electronic voting technologies, although the exact advantages and disadvantages will depend on the electoral environment and the electronic voting solution being implemented. The following section will elaborate on the examples from other countries which have tried electronic voting and then decided to discontinue its use. These examples can be very instructive for any countries wishing to pursue electronic voting. Finally the section will conclude with a discussion of emerging trends that can be seen in the global use of electronic voting.

[79] See Figure 13 below.

[80] Approximately 15 cases were excluded on this basis, even though some of these cases might be well advanced in their consideration. However, it would be very difficult to include a review of countries which are considering the use of voting technologies as it is difficult to measure the seriousness with which these technologies are being considered. The conduct of a binding political vote is a concrete benchmark which can be objectively determined.

2000 U.S. Presidential Election – A Defining Moment

The U.S. was the first country to adopt voting technology with mechanical voting machines, introduced in 1892. It was also amongst the group of countries which sought to adopt electronic voting machines when they started to become available in the 1970-90s. In trying to understand the U.S. approach to voting technology it is important to note that the administration of elections is highly decentralized. While needing to remain within broad electoral standards defined at the federal level, many of the important details concerning the way in which elections are administered are left to the state or even the county to determine.

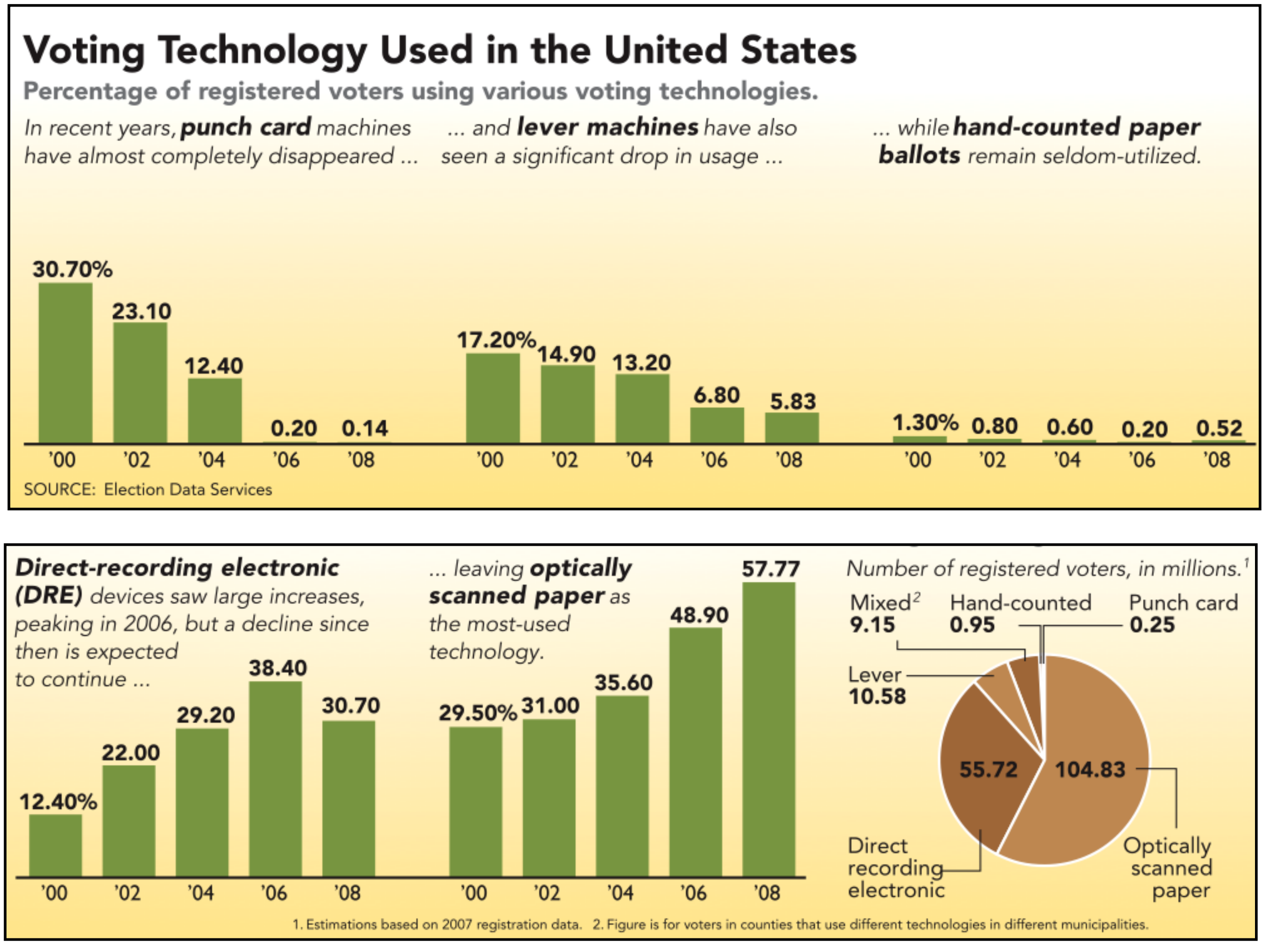
This leads to a very fragmented picture of election administration practices in the U.S., and this is certainly the case when it comes to the adoption of election technologies. As can be seen from Figure 7, at the time of the 2000 presidential election, punch card voting and counting and lever voting machines were used by nearly 48 percent of the electorate. Direct recording electronic voting machines and the optical scanning of paper ballots were used for 12.4 percent and 29.5 percent of the electorate, respectively. Only 1.3 percent of the electorate used hand-counted paper ballots.

In many ways the discourse on electronic voting has been defined over the past decade by events in the troubled 2000 U.S. election. In this election, 25 Electoral College votes from Florida were declared for George W. Bush and effectively decided the election in his favor. However, voting and counting in Florida was plagued by irregularities, which due to the small majority in Florida for Bush, (initially declared to have won by 1,784 votes) could have changed the presidential election result.

These irregularities included the removal of 94,000 voters from the electoral roll, many incorrectly identified as felons. The removals were skewed towards African American voters, who were statistically highly likely to have voted for Bush's opponent, Al Gore (Dieter 2003). Ballot design was also an issue. In Palm Beach the infamous "butterfly ballot" was thought to have caused a significant number of votes (more than 2,000) to be misdirected from Al Gore to independent candidate Patrick Buchanan (Wand 2001). In Duval County, a more traditionally Democrat County, incorrect ballot instructions led to over 50,000 overvotes (multiple selections for the same election, and therefore ballots considered as invalid) for president (Mebane 2004).

Florida used punch card technology for its ballots, as did many other states in the U.S. at the time, and the votes rejected by the counting machines proved to be very controversial. Enduring images exist of electoral officials inspecting punch card ballots with magnifying glasses to see if the intention of the voter could be determined. New phrases burst into the political discourse. Voters became aware of the difference between "hanging chads," "swinging chads" and "pregnant chads," and the consequences for vote ballot validity.

Figure 7 – Voting Technology Used in the United States



Source: Election Data Services, see their website http://www.electiondataservices.com/ [last accessed 5 November 2011]

The recounting of these rejected ballots was seen as potentially determinative of the overall presidential election result, leading to protracted legal challenges whether to recount these ballots or not. These legal challenges went all the way to the Supreme Court, which split along partisan lines in its 5-4 divisive decision to stop the recount that had been taking place on the instruction of the Florida Supreme Court. This decision finally paved the way for the Florida Secretary of State to declare the results of the presidential election for Florida on 9 December, and for the overall presidential election result to be finalized.

One of the consequences of the events in Florida in 2000 was that the 2002 Help America Vote Act (HAVA) legislated the replacement of punch card and lever-based voting systems. In many cases states and counties replaced this old technology with voting and counting machines. However, election technology was suddenly under the public spotlight. Public opinion understandably turned against the use of punch card voting. Technology was meant to assist the voting process, not obscure and confuse it. The implicit trust that had previously existed about the use of voting technology in the U.S. was severely damaged by the events of 2000. Subsequently the operation of election technology has been much more heavily scrutinized and any deficiencies exploited by the growing ranks of those opposed to electronic voting.

While these events directly relate to the U.S. experience of voting technologies in the last decade, they have resonated through many other countries, especially in Europe, and led to a more skeptical approach to technology in these countries. As can be seen from Figure 7 above, the use of punch card voting and counting reduced significantly after the 2000 election, until by 2006 it was hardly in use at all. Likewise, the use of lever machines also reduced, but less so, and by 2008 only about nine percent of the electorate were still using these mechanical machines.

The main beneficiary of this move away from older technologies was initially electronic voting machines, whose use in the U.S. increased more than three times, to 38 percent, by 2006. The use of optically scanned paper ballots also increased in this period, from 29 percent to 49 percent. What we see from this point onwards though is a reduction in the use of electronic voting machines and further increases in the use of optically scanned paper ballots, up to nearly 58 percent by 2008. This shift away from electronic voting machines was due to growing distrust in the use of these machines, especially because no voter verifiable audit trail existed for the majority of the machines used. Combined with some damning reports on the security of certain electronic voting machines and examples of software errors in voting systems in use (Kohno et al 2004: 27, Feldman, Halderman and Felton 2007, Bannet *et al* 2004, Harris 2004) this led to even greater levels of skepticism towards electronic voting machines in the U.S.. This U.S. experience provides a frame of reference within which to view many other country's electronic voting experiences.

Overview of International Experience

The results of this global study of electronic voting experiences are displayed on the map of global electronic voting experiences (Figures 9 and 10) and also detailed in Figure 8, below.

Thirty countries were found to have met the criteria of using electronic voting machines in a binding vote of a political nature. Nine countries piloted electronic voting and then discontinued use. In seven countries these pilots are still ongoing. In 11 countries electronic voting machines are currently being used and in three of these countries they are used nationwide rather than just for parts of the electorate. An additional three countries have formally discontinued the use of electronic voting machines.

The regional breakdown of this data is also interesting, especially in Europe where there are eight[81] examples of electronic voting, but in the vast majority of these examples electronic voting is no longer used. In four cases electronic voting was piloted and not continued (Ireland, Italy, Norway and the UK) and in two cases the use of electronic voting machines has been discontinued (the Netherlands and Germany[82]). Only two countries in Europe are currently using electronic voting machines (Belgium and

[81] Nine if Russia is considered as in Europe and not Asia.

[82] For more details of these cases see the chapter on electronic voting experiences and the section on countries which have discontinued the use of electronic voting.

France) and in neither case are they being used nationwide.[83] In fact in France they are used in very few cities.[84] This limited use of electronic voting machines has been influenced by the U.S. experiences of the 2000 presidential election, and also the decisions of some European countries to specifically not continue with electronic voting (Ireland, the Netherlands and Germany) on the basis of security and transparency concerns.

[83] Three if Russia is included. Russia is categorized as having ongoing pilots.

[84] In the 2007 Presidential Election electronic voting was only used for 3 percent of the electorate.

Figure 8 – Countries Using Electronic Voting[85]

Country	Category
Argentina	Currently used in some parts of the country
Australia	Piloted and Not Continued
Belgium	Currently used in parts of the country
Bangladesh	Pilots Ongoing
Bhutan	Pilots Ongoing
Brazil	Currently used Nationwide
Canada	Currently used in some parts of the country
Costa Rica	Piloted and Not Continued
Ecuador	Pilots Ongoing
France	Currently used in parts of the country
Germany	Discontinued
Guatemala	Piloted and Not Continued
India	Currently used Nationwide
Indonesia	Pilots Ongoing
Ireland	Piloted and Not Continued
Italy	Piloted and Not Continued
Japan	Currently used in parts of the country
Kazakhstan	Piloted and Not Continued
Mexico	Currently used in some parts of the country
Mongolia	Pilots Ongoing
Nepal	Pilots Ongoing
Netherlands	Discontinued
Norway	Piloted and Not Continued
Paraguay	Discontinued
Peru	Currently used in some parts of the country
Philippines	Piloted and Not Continued
Russia	Pilots Ongoing
United States	Currently used in parts of the country
Venezuela	Currently used Nationwide
United Kingdom	Piloted and Not Continued

This limited use of electronic voting in Europe contrasts sharply with trends seen in South America and Asia, where not only is the use of electronic voting more prevalent at the moment but there is greater interest in future adoption of these technologies. Of the three examples where electronic voting is used nationwide for elections, two are in South America (Brazil and Venezuela) and one is in Asia (India).

[85] Data presented in figures 8, 9 and ten has been collected from many different sources, including sources such as reports from election management bodies, observer reports, other overviews of internet voting (e.g. EAC 2011), the ACE Website and direct contacts with election management bodies.

Figure 9 – Electronic Voting Usage Globally

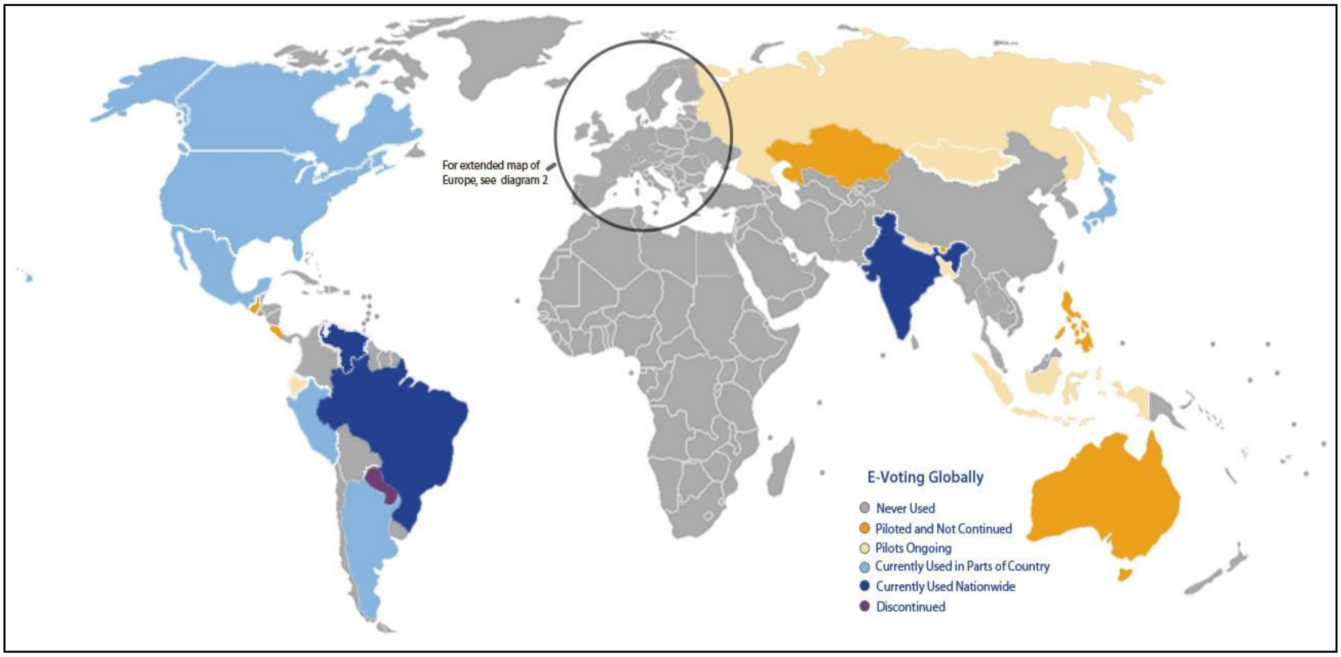
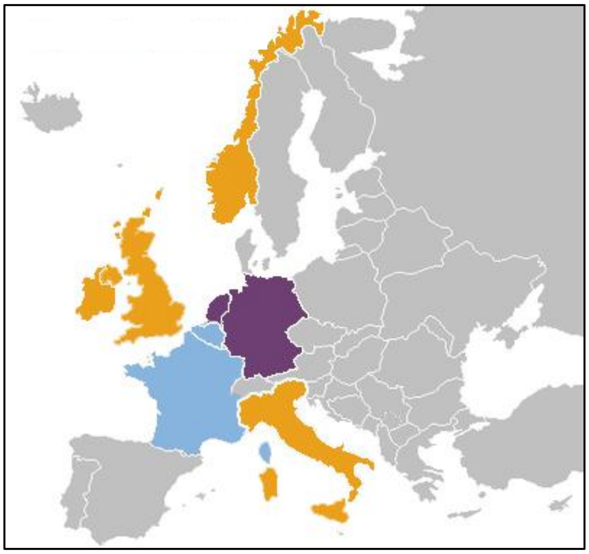

For extended map of Europe, see diagram 2
E-Voting Globally
● Never Used
● Piloted and Not Continued
● Pilots Ongoing
● Currently Used in Parts of Country
● Currently Used Nationwide
● Discontinued

Figure 10 – Electronic Voting Usage Globally



Brazil and India are both highly influential countries globally and even more so within their respective continents. Both countries have been using their electronic voting machines for over a decade now and have seen significant benefits in the quality of their elections as a result. This is not to say that there is not opposition to the use of electronic voting machines in these countries, but opposition has, so far, failed to gather much momentum.[86] Both countries also actively market their voting machines with neighboring countries, sometimes offering to loan them for free. This advocacy of the benefits of electronic voting by such influential global and regional powers may be one of the factors accounting for these trends in South America and Asia.

Another regional trend is that electronic voting has not made any inroads into the African continent to date, with zero cases of electronic voting. With a large number of poor countries on the continent many of these countries would struggle to find the finances necessary for the significant initial investment that is required to implement electronic voting. Not all countries in Africa are too poor for such investment, however, and there are other good reasons why electronic voting may not have made inroads into

[86] Although a recent report into possible security flaws in the Indian voting machines have increased calls for voting machine which are more verifiable – see (Prasad *et al* 2010).

Africa. Electronic voting machines rely on certain infrastructure features, such as power and communications, which are not available nationwide in many countries in Africa. In addition, Africa has some extreme climatic conditions – heat, humidity and dust – which electronic voting machines are only recently being designed to withstand.

In addition to this review of global trends, six cases of electronic voting were reviewed in depth for this assessment. Two cases, India and Brazil, represent large democracies which have adopted electronic voting for their elections and use them nationwide. A third case, the U.S., has been at the forefront of election technology adoption, being the first to use electronic voting machines in 1975. As there are many electoral jurisdictions in the U.S., one typical jurisdiction using electronic voting, Maryland has been selected for in depth review. Three European cases were also selected. The Netherlands was an early adopter of election technology, but decided in 2007 to discontinue the use of all voting technology. Belgium was also an early adopter of electronic voting and continues to use it in the majority of the country. France uses electronic voting, but only in a small percentage of the population.

A brief summary of each case is provided here, highlighting interesting aspects of each case. The full data sheets are annexed to this report.

- Belgium – adopted electronic voting machines early, first using them in 1991. The reasons for adoption included anticipated cost savings, quick delivery of results and easier administration. Voting machines have been used increasingly since they were introduced and are now used for about 44 percent of the population, although there is a significant difference in the use of a voting machine between the Flemish and Walloon regions.87 Voting machines are used for all elections in the jurisdictions which have chosen to use them – local, regional, federal and European.
- The Belgian system is unique when compared to other countries using voting machines, in that although a voting machine is used to select ballot choices, the voting machine does not store the vote. Belgian voters are provided a magnetic card which they insert into the voting machine and the voting machine writes the ballot choice selected by the voter onto this card. The card is then put into an electronic ballot box which counts the vote on the card as it is placed in the ballot box.
- At the end of polling the electronic ballot box delivers the results. It is possible to have the ballot box recount the ballots (magnetic cards) in order to check the results. The magnetic card also acts as a voter verifiable audit trail in that in each polling station there are multiple voting terminals. The voter can place the magnetic card in another voting terminal to read the ballot which has been cast (but not change it) and check that it has recorded the vote correctly before placing it in the ballot box.
- The Belgian system has been changed little since its initial development in the mid-1990s and relies on some technology which is now almost obsolete (such as floppy discs). The Belgian Government is in the process of procuring new voting machines and in the summer of 2011

[87] 49 percent of Flemish voters are using voting machines, only 22 percent Walloon voters do so. Brussels has completely substituted paper means by voting machines.

signed an initial contract with a supplier to develop a prototype voting machine which meets its new specifications. This new voting machine was trialed in non-political elections in October 2011.88

- Brazil – had a long but troubled history of democracy, with the first parliamentary elections taking place in the 1820s. Elections had been plagued with fraud (Ribeiro de Souza (no date)) and poor levels of participation. In 1995 the Supreme Electoral Court created a task force financed by the World Bank to find a way to stop fraud and strengthen political participation in a country where the illiterate population represented 30 percent of the population. Electronic voting machines were the recommended solution (Avgerou et al 2007:6).
- Trials of the electronic voting machine began in 1996, with nationwide implementation in 2000. Brazil is the first country to have deployed electronic voting machines nationwide for elections, and the machines are used for all elections. Electronic voting succeeded in both reducing fraud and enfranchising illiterate voters. While the rate of invalid votes averaged 40 percent before electronic voting, it went down to 7.6 percent in 2002 (Avgerou et al 2007:9).
- The Brazilian voting machine consists of two terminals, the first is used by the polling official to authenticate the voter and the second is used by the voter to cast a ballot. Authentication consists of the polling official typing in the ID number of the voter. If the voter is found and able to vote then the polling official activates the voting terminal. The voting terminal consists of a numerical keyboard and an LCD screen. Voters enter the number of the candidate for whom they wish to vote. The selection is displayed and the voter can confirm the choice or alter it. The voter can also cast a blank ballot. At the end of polling the voting machine produces the results from the polling station. These results are also encrypted and loaded onto a diskette which is taken to a results consolidation center (Avgerou et al 2009: 141-2).
- The current Brazilian voting machines do not have a voter verifiable audit trail; attempts to introduce a paper trail trialed unsuccessfully in 2002. In 2009, the Brazilian parliament reintroduced the obligation of a paper trail which was to be implemented by 2014. However, in November 2011 the Committee on Constitution and Justice of the Senate approved a bill that revokes this requirement on the basis that it could violate the secrecy of the vote.89
- France – first introduced electronic voting machines in 2004. According to explanations provided by the electoral authorities, organizational issues led to this decision because it would have been increasingly difficult to recruit enough people to conduct electoral procedures in each polling station. E-voting seemed to ease those organizational needs. The municipalities which use electronic voting machines account for approximately 3 percent of the electorate, and use the machines for all levels of elections.
- Voting machines in France have to be certified for use by the federal government, and currently three different systems are certified. These systems vary in functionality, but follow the model of a voting machine which the voter uses to cast a ballot and which stores the ballot choices

[88] See http://www.ibz.rrn.fgov.be/index.php?id=3011&L=0 [last accessed 5 November 2011].

[89] See http://www.fraudeurnaseletronicas.com.br/2011/11/senado-revoga-obrigatoriedade-de-urna.html and http://www.fraudeurnaseletronicas.com.br/2011/10/stf-revoga-lei-do-voto-impresso-e.html [both last accessed on 22 February, 2012].

made, producing results at the end of polling. None of the certified systems includes a voter verifiable audit trail.

- India – in the 1970s the electoral process in India was confronted by three main problems, made more challenging by the sheer size of the country: logistics, empowerment of illiterate voters and recurrent vote rigging. Vote rigging consisted of ballot boxes disappearing and reappearing full of illegitimate ballots, of voters turning up at the polling station to discover that they had already voted, of trucks carrying sealed ballot boxes being hijacked on the way to the tallying center and thugs invading polling stations, stuffing the ballot boxes and chasing all the voters away. In every election since independence in 1947, the number of invalid votes (linked to illiteracy) was more than the winning margin between candidates.
- Electronic voting machines put an end to these problems. They were first used in 1982 in the Parur Assembly Constituency of Kerala in 50 polling stations. The deployment of voting machines progressed slowly, as their use and impact was being tested. The 2004 General Election was the first time that Indian voting machines were used nationwide.90
- The voting machine is made of two devices running on 6-volt batteries. One device is the voting unit, the other is the control unit operated by the electoral officer. They are connected by a five-meter cable. The voting unit has one button per candidate (16 buttons on the unit, although it is possible to link up to 4 units to accommodate 64 candidates). The candidates' name and party symbols are displayed next to the corresponding button so that illiterate people can vote easily.91
- Machines can only record five votes per minute to avoid ballot stuffing by thugs invading the polling station.92 After the vote, voting machines are brought to counting centers, where the outcome of the election is tallied. In the 2009 general election, 1.378 million voting machines were used.
- No audit trail is available with the Indian voting machine. However, growing calls from citizens and political parties for means to verify the accurate functioning of the voting machine has increased pressure on the Election Commission of India to provide this audit trail (Prasad et al 2010). Responding to this pressure, new voting machines with a paper audit trail were piloted in 200 polling stations in July 2011.93
- The Netherlands – made provisions in its electoral law as early as 1965 authorizing the use of technology to support the voting and counting processes. Initially this was used to develop counting technology, but from the early 1990s the Netherlands began to implement electronic voting technology. The use of this technology spread rapidly throughout the Netherlands and, by 2006, 97.7 percent of Dutch municipalities were using electronic voting machines.
- Two voting machines were used in the Netherlands, one touch screen and one button operated. There was no voter verified audit trail available with either machine. Opposition to the use of

[90] See http://eci.nic.in/eci_main1/evm.aspx [last accessed on 22 February, 2012].

[91] See EVM PowerPoint Presentation on the Indian Election Commission website - http://eci.nic.in/eci_main1/presentation.aspx [last accessed on February 29, 2012].

[92] See EVM FAQs on the Indian Election Commission website - http://eci.nic.in/eci_main1/evm.aspx [last accessed on February 29, 2012].

[93] See http://www.youtube.com/watch?v=EJnTy_ZNEJw [last accessed on 22 February, 2012].

these voting machines had been growing since 2000, but in 2006-7 civil society groups proved that some serious security flaws existed with the voting machines being used and that it was possible to remotely monitor the way in which voters voted through the emissions from the voting machine. After a review by the government of these concerns in 2007, the government decided to return to paper balloting. More can be read about the Netherlands case later in this report.

- United States of America - State of Maryland – decided to review its voting system after the disputed 2000 presidential election. The committee tasked with this review recommended state-wide electronic voting. In 2001, Governor Glendening signed House Bill 1457, which required a uniform system to be used across all counties in the state, unlike many other states where counties can choose their voting systems. Electronic voting machines were implemented for the 2002 election and have been used ever since. In fact Maryland bought Diebold electronic voting machines, whose source code was analyzed by Avi Ruben and his research colleagues to reveal serious security flaws (Kohno et al 2004: 27).
- Since 2006, Maryland also uses electronic poll books which are used to identify voters and cross them off the register as having voted. Once voters have been authenticated on the electronic poll book they are provided a one-time activation card for the voting machine. This card is then inserted into the voting machine and the ballot appears on the touch screen with all electoral races available to that specific voter. Once the ballot is cast, the activation card is erased and ejected from the voting unit. The activation card is then returned and is available for use with another voter. After polls have closed, a poll worker inserts an administrator card into each voting machine and puts the machine into a post-election mode where it will no longer record votes. The machine then copies the data onto the card, which is taken to a central tabulation facility.
- At the moment, there is no paper trail for the voter. In 2005, the Maryland General Assembly passed Senate Bill 849 and House Bill 479, which required the State Administrator of Elections to conduct a study of independent verification systems. Governor Robert L. Ehrlich, Jr., however, vetoed the legislation. In 2007, Governor Martin O'Malley signed into law, SB 392, which called for replacing Maryland's paperless touch-screen voting system with a system that produces a paper record. The transition, however, was delayed after the State Board of Elections estimated that the cost of the switch would be too high.

Technical Comparison of the Six Case Studies

The case studies of electronic voting selected for this report, which are indicative of other electronic voting systems, have far fewer security and quality assurance features than comparative Internet voting systems. This is in part because these electronic voting systems are used in a polling station environment, where some of the security and quality assurance mechanism are performed by the polling station staff.

For example, almost all electronic voting systems rely on polling staff to authenticate the voters, normally by verifying their identity and presence on the electoral register for that polling station. Only in the case of Brazil is the electronic voting machine used to ensure that no voters cast multiple ballots, with the voter's registration number being entered into the voting machine. Elsewhere this control is conducted through the manual maintenance of an electoral register by polling staff. This situation is likely to change in the future, and voting machines are being developed and trialed recently that will also biometrically authenticate the voter against a preloaded electronic electoral register.

Mechanisms for vote storage vary considerably between voting machine suppliers and the procedures implemented by the EMB. Few systems contain alternative vote storage mechanisms, meaning that in the event of serious voting machine failure votes are likely to be lost. However, some voting machines (for example the Indian voting machine) store the vote information on multiple storage locations within the machine. The use of voter verified paper audit trails also provides a form of backup for vote data in the event of machine malfunction. Belgium is an unusual case with respect to electronic voting in that the system that it has used since the 1990's creates a token (the vote is stored on a magnetic card) which is read by the electronic ballot box. The token can always be used again to create the results if there is a malfunction with the ballot box.

None of the six voting system case studies provide voters with a receipt for the voting transaction, and this is standard across other electronic voting machine solutions. Of the six case studies, only the Belgium system (which is in the process of being replaced) has any form of voter verifiable audit trail. The magnetic card which the voter uses to cast a ballot on the voting machine, and stores the vote itself, can be inserted into any other voting machine in the polling station to confirm the vote that it has stored as a result of the voting transaction. While this is a technical possibility, it is one that is rarely used so may be more theoretical than actual. The situation is changing though, and India, Brazil and the USA have all indicated an intention to implement voter verifiable audit trails in the future. In some cases these solutions have already been trialed. Belgium is also in the process of replacing its existing system with a more modern system which includes a voter verifiable audit trail.

General Benefits of Electronic Voting Machines

While the specific benefits offered by an electronic voting system will depend on the electoral environment and on the specifics of the electronic voting system implemented, it is clear that electronic voting has many potential benefits to offer over paper balloting. Based on the experiences of electronic voting to-date, the following kinds of benefits can be achieved by using electronic voting:[94]

- **Ability to Deal with Complex Elections** – electronic voting technologies are generally able to deal with complex elections easily. This includes more complex electoral systems, such as preference and block voting, as well as holding multiple elections at the same time (e.g., concurrent presidential, parliamentary and local government elections).
- **Accessibility** – electronic voting technology can have an impact on ballot accessibility. It may make the process more engaging to groups which are computer literate (e.g., young voters), but also make voting more feasible for voting groups which currently struggle to participate in the process, especially persons with disabilities. Voting machines can be specifically designed to make voting possible for voters with disabilities in such a way that they do not require

[94] This list was adapted from (Goldsmith 2011).

assistance (which they often do with paper ballots); therefore protecting the secrecy of their vote.

- **Less Polling Staff** – with a simpler process in the polling station, no ballot to be issued and no ballot box to monitor,95 it may be possible to reduce the number of staff required for each polling station. It is sometimes difficult to find staff for polling stations so this may be a significant benefit. Where the technology also counts the ballots, it means polling staff will not need to work as long on Election Day.
- **Elimination of Invalid/Incorrectly Cast Ballots** – in some countries significant numbers of ballots are deemed invalid and not counted. Those voters are disenfranchised. Where ballots are cast and recorded electronically, the electronic voting software can be configured to ensure only valid ballots are cast (although blank ballots may still be allowed).
- **Speed of Counting** – an important advantage of using electronic voting technology, which directly records votes electronically, is that results are immediately available after polls close, without a lengthy counting process.
- **Standard Adjudication of Ballots** – counting paper ballots electronically ensures that the same kind of ballot marking is adjudicated in the same manner across all polling stations. This ensures consistency on which ballots are valid and which are determined to be invalid. This is often not the case with manual counting of ballots.
- **Accurate Tabulation of Results** – when results are electronically recorded and transmitted to the EMB for tabulation, the possibility of data entry errors during results tabulation is greatly diminished.
- **Fraud Prevention** – electronic voting technologies can mitigate some fraud in polling stations. For example, some electronic voting technologies only allow votes to be cast at a certain speed, thus mitigating ballot stuffing. Similarly, the fact that electronic voting machines tabulate the results mitigates fraud during the counting process, although it must be noted that the use of electronic voting machines opens up new possibilities for fraud.

General Disadvantages of Electronic Voting Machines

The use of electronic voting machines also presents new challenges and potential problems, and these are listed below:

- **Lack of Transparency** – Transparency is a key component of building and maintaining trust in the electoral process. The paper balloting system is very transparent. Observers can watch ballots being issued, voters placing their marked ballots in the ballot box and ballots being counted. Electronic voting technology, more so than electronic counting technology, is often considered to be a ‘black box.’ This is because it is not possible to observe the way in which the selected choices of voters are aggregated to produce the results announced. We simply have to trust that these results accurately reflect the choices made by voters. This makes the checking of results produced by electronic voting and counting technologies all the more important.

[95] Although some electronic voting solutions still have a ballot box, such as the old systems in Belgium.

- **Confidence** – Lack of transparency with electronic voting technologies means that confidence in the operation of the technology is a considerable problem. Election management bodies need to ensure that trust in the electoral process is maintained. While the introduction of electronic voting technologies does not have to lead to an erosion of trust in the electoral process, it has happened in some countries. Election management bodies are likely to have to introduce new procedures, possibly random audit of results or publication of source code for electronic voting and counting technologies, in order to maintain trust in the process.
- **Audit of Results** – A great strength of the paper balloting system is that if the results of an election are challenged then the ballots can be recounted to check the result. Many electronic voting machines96 have no such possibility for auditing and checking the results of an election. The ability to audit and check is an important feature of building trust in the electoral process and increasing acceptance of the results. Some electronic voting machines do have a VVPAT, which prints a copy of the electronic ballot and is verified by the voter before casting the ballot. This VVPAT can be used to audit/check electronic results produced by the electronic voting machine (EVM). The provision of a VVPAT is increasingly seen as a standard for EVMs,97 but the inclusion of a VVPAT does have cost and logistic implications.
- **Secrecy of the Ballot** – A key international standard for elections is that it should not be possible to determine how an individual voter has voted. Electronic voting technologies can undermine this secrecy. With some VVPAT systems, but not all, the order of ballots cast is clear from the paper audit trail. If the order of voters is recorded by observers/party agents then the way in which voters voted can be determined. Also, electronic voting systems which identify the voter first (as all remote electronic voting systems must do) provide the possibility for, but not the necessity of, linking the voter to the ballot cast.
- **Setup Procedures for Electronic Voting Machines** – Procedures that need to be conducted at the beginning and end of polling may be difficult for Presiding Officers, who may not be sufficiently technology literate to understand and implement them.
- **Tendered Ballots** – Some countries allow voters not on the voter register or who are thought to have voted before to cast a ‘tendered ballot’, ‘conditional ballot’ or ‘challenged ballot’ which will only be counted in certain circumstances. Most electronic voting technologies do not allow the casting of such ballots as any vote cast will be included in the results. While it is possible that electronic voting technologies could be adapted to cater for these types of ballots, it adds a level of administrative complexity which may outweigh the benefit.
- **Consequences of Breakdown** – If an electronic voting machine breaks down before or during polling and it is not possible to fix it, the potential consequence is disenfranchisement of the voters in that polling station. This is a serious consequence which would require that spare electronic voting machines be available at a local level in order to cope with any breakdowns. The need for stand-by voting machines and the logistical arrangements to cover this would increase the cost of introducing electronic voting technologies.

[96] Electronic counting machines have the paper ballot completed by the voter as a natural audit trail.

[97] The Council of Europe requires that the correctness of the result produced by an e-voting system should be verifiable and that the system should be auditable – recommendations 26, 59 and 100-110 (Council of Europe 2004).

- **Confusion for Illiterate/Uneducated Voters** – Any change in a system can cause confusion since users of the system have to adapt to new procedures. Electronic voting technologies, while simple to use for most educated voters, may be confusing for illiterate and poorly educated voters. While this is a genuine concern, it is worth noting that simpler electronic voting solutions have been successfully used for populations with high levels of illiteracy.
- **Voter Education** – A considerable amount of voter education would be required to educate and prepare voters for a move to electronic voting technology. This voter education exercise would likely be costly.
- **Specialized IT Skills** – Maintenance and repair of hardware used by electronic voting technologies requires specialized IT skills which may or may not be available in sufficient supply and at a reasonable cost in the local labor market. These skills may be required centrally as well as at the local level in order to deal with problems closer to Election Day when voting machines have been distributed. If these skills are in short supply then the use of electronic voting technologies may be unsustainable.
- **Integrity and Accuracy of Source Code** – Electronic voting technologies rely on software to function. This software is a set of instructions to the electronic voting system defining how it operates. As with any set of instructions, mistakes can be made and a thorough review of the source code has to be conducted before using any electronic voting technologies. As it takes specialized technical skills to be able to read and understand source code, an independent testing authority may be required to review any electronic voting system. This review would determine, to the greatest extent possible, whether the system is functioning according to its specifications and whether the system performs sufficiently well before it is accredited for use in an election.
- **Storage of Equipment** – Some electronic voting system hardware is required to be stored under temperature controlled conditions between elections. Temperature controlled storage may be difficult and costly to find, especially on a regional/local basis.
- **Environmental Considerations** – Electronic voting hardware, especially the machinery, may be required to withstand, and perform reliably, under a wide range of environmental factors including extreme heat, cold, humidity and dust. Finding electronic voting solutions which reliably operate in such situations may be difficult.
- **Power Considerations** – Electronic voting technologies require a source of power, with most running on mains electricity. For solutions based in polling stations, chronic power shortages or the lack of electricity entirely could require electronic voting or counting machines to run for the entire period of polling on an alternative power source. Such power requirements limit the options available.
- **Security** – Different security challenges are presented by electronic voting technologies compared to paper balloting systems. For example, electronic transmission of results for tabulation presents the possibility for the system to be hacked and false results inserted. Secure systems of protection and verification for electronic data need to be ensured.
- **Consequences of Fraud** – While fraud conducted using the paper balloting system is often localized and not widespread, the possibility exists with electronic counting technologies for

fraud to be implemented on a nationwide scale. Electronic voting software could be manipulated to record vote preferences which are different from those made by the voters, or fraud and manipulation could occur in the electronic tabulation of results if such tabulation occurs directly from the electronic voting machines.

- **Management Complexity** – Managing the introduction, testing, deployment, retrieval and security for electronic technologies can be more complicated than managing a paper-based election. Election management bodies often lack adequate experience in management of such complex systems. This can lead to a heavy reliance on the technology contractor to the point of surrendering control of the electoral process to an outside entity.
- **Cost** – The cost of electronic voting machines ranges from $300 per unit for the more simple solutions to approximately $5,000 per unit for more complex solutions. When aggregated for an entire election this can represent a potentially huge investment for many countries, although a full comparison against the costs of paper balloting needs to take into consideration the life cycle of electronic voting technologies and the number of election cycles they would be expected to cover.

The examples where electronic voting has been discontinued can be instructive of seeing how these challenges and problems can become important, if not critical, factors for countries implementing electronic voting machines.

Cases of Discontinued Use

There are three cases where the use of electronic voting machines was discontinued – Germany, the Netherlands and Paraguay. The background and reasons for these decisions will be reviewed here. In addition to these, the case of Ireland is also reviewed. Although it is categorized as a case where electronic voting was piloted and not continued, this obscures the peculiarities of the Irish case. While the categorization is accurate, in that Ireland had conducted a small pilot of electronic voting and then did not proceed with full scale implementation, this obscures the fact that Ireland had procured the electronic voting machines required for full scale implementation of electronic voting at the time of the decision not to use them. Therefore in many ways the Irish case is more similar to those in which electronic voting was discontinued.

These cases of discontinued use of electronic voting are dealt with in chronological order, starting with Ireland. The following section, on emerging trends, will look at what lessons we can learn from these critical examples of electronic voting.

Ireland (2004)

The Irish government began investigating the possible use of electronic voting machines in 1998 but it took until 2002 for electronic voting trials to be conducted. After these trials a decision was taken by the government to implement electronic voting nationwide in the June 2004 European and local elections, with voting machines being procured from NEDAP, a Dutch company, for €53 million.

However, throughout 2003, opposition grew from civil society and some political parties to the government decision to implement electronic voting. In response to this growing pressure, on March 1, 2004 the government established a Commission on Electronic Voting to report on the secrecy and accuracy of the selected electronic voting system, to review the tests conducted on this system and to make a recommendation on the suitability of the system for use in the June 2004 elections.

The Commission's Interim Report[98] published on 29 April 2004 sent shockwaves through the Irish government by finding that it was, "not in a position to recommend with the requisite degree of confidence the use of the chosen [electronic voting] system at elections in Ireland in June 2004" (Commission on Electronic Voting 2004a: 8). This was due to concerns about the accuracy of the system due to insufficient testing and the fact that changes were still being made to the system, not providing sufficient time to retest the system before its planned use. Concerns were also raised about possible violations of vote secrecy caused by the beeping of the machine and plans to publish full details of all votes cast (lower order preferences under Ireland's single transferable vote electoral system potentially providing a signature for the voter).

The Irish government was left with no choice but to cancel the planned use of its electronic voting machines in the 2004 elections. A first report issued by the Commission on Electronic Voting in December 2004 re-iterated the conclusions and recommendations of the Interim Report. It made an additional observation that the voting machines did not have a voter verified audit trail. It said that an audit trail would help audit and build trust in the voting machines, and that in its absence even higher standards of testing were required (Commission on Electronic Voting 2004b).

The status of electronic voting in Ireland entered a limbo phase after these initial reports of the Commission. The Irish government still wished to pursue the use of electronic voting machines, but could not do so against the recommendation of the Commission. The cost of augmenting the voting machines to make them compliant with the Commission's recommendations was estimated to cost a further €28 million (McDermott 2010: 72), and this additional expenditure was seen as politically unpalatable.

A Second Report by the Commission in 2006 put another nail in the coffin of electronic voting in Ireland. Elaborating many of the previous findings and adding sections on physical and operational security, and compliance with Council of Europe recommendations on electronic voting, the Commission found that:

> *"When compared in terms of secrecy and accuracy, the existing paper system is moderately superior overall to the chosen electronic system as currently proposed for use in Ireland (and in some respects only marginally so). However, the Commission's work has highlighted modifications to the chosen system and the procedural arrangements for its deployment, together with further software analysis and testing of the system as a whole that could potentially remedy this situation." (Commission on Electronic Voting 2006: 14)*

This measured language of the Commission was seen by many as a damning indictment of the chosen electronic voting system (McDermott 2010: 77). A formal government decision to end the electronic voting project did not come until April 2009, when the Minister for the Environment, Heritage and Local

[98] See the Commission's website for this report and all other reports - http://www.cev.ie/ [last accessed on October 28, 2012].

Government announced that the government had decided not to proceed with the electronic voting project and a decision would be taken on the disposal of the voting machines.[99]

Netherlands (2007)

The Netherlands was one of the first countries to embrace voting and counting technologies. The 1980s saw the Dutch attempting to automate the counting process with the first electronic voting machines appearing in the early 1990s. From 1994 the Dutch government started to actively promote the use of electronic voting machines (Jacobs and Pieters 2009: 124). By the 2006 election 97.7 percent of municipalities were using them.

Criticisms of the use of electronic voting machines in the Netherlands started from 2000, with the main concerns being the secrecy of the source code and evaluation reports, and the lack of verifiability of the machines. However, it took developments in Ireland, which were using the same NEDAP machines as the majority of the Netherlands and the introduction of voting machines to the city of Amsterdam, to bring these concerns to fruition.

Developments in Ireland led Dutch citizens to start asking similar questions about the suitability of the machines for their own country. In 2006 a pressure group called “We don’t trust voting computers” was established. The group managed to buy some NEDAP machines and identified in them a number of security flaws, including the easy replacement of program chips allowing the results to be manipulated. Due to the lack of verification mechanisms such replacement would go unnoticed. The group also demonstrated the susceptibility to eavesdropping on radio emissions of the voting (called the “tempest attack”).

In 2006, the government established two committees to look into the issue of electronic voting. In April the Voting Machines Decisions Committee issued a report entitled *Voting Machines, a neglected dossier*. The report listed recommendations for both the short and medium terms about voting machine legislation. Autumn 2006 saw the publication of a report, *Voting with confidence*, issued by the Advisory Committee on the Voting Process Mechanism, after which the cabinet adopted a position on the matter.

The Advisory Committee’s report recommended that due to issues of transparency and verifiability, voting should take place using only paper ballots in polling stations, effectively ending the Netherlands’ use of electronic voting machines. While the Committee’s report did not rule out the possibility of electronic voting machines in the future, which better met the requirements of elections in the Netherlands, there have been no moves to introduce new electronic voting machines since.

In October 2007 the regulation allowing the use of electronic voting machines was withdrawn.

Paraguay (2008)

Paraguay first experimented with the use of electronic voting machines in 2001 through an agreement between the Paraguayan Supreme Electoral Court of Justice and the Supreme Electoral Court of Brazil, which loaned a small number of Brazilian voting machines for trials in local government elections. In 2003, this agreement was extended with 6,000 voting machines being provided for the presidential and

[99] See http://www.environ.ie/en/LocalGovernment/Voting/News/MainBody,20056,en.htm [last accessed 3 November 2011].

parliamentary election, an election where over 50 percent of voters used electronic voting machines.[100] This cooperation was further extended for a series of local elections in the following years, with 16,000 voting machines being loaned to Paraguay[101] and the majority of voters casting ballots using these machines.

Throughout this period, however, opposition from political parties had been growing. As a result, the Supreme Electoral Court of Justice requested the opinions of political parties concerning the future use of electronic voting machines. The majority of opposition political parties opposed the use of electronic voting machines, favoring paper voting. The ruling party only preferred the use of electronic voting machines but did not object to the use of paper ballots. Therefore the decision was taken that the general elections to be held in 2008 would be done solely using paper ballots.[102]

Germany (2009)

In 1998 the first electronic voting machines, supplied by the Dutch supplier NEDAP, were trialed in Cologne. The trial was seen as successful and one year later Cologne used electronic voting machines for its entire European Parliament Election (Commission on Electronic Voting 2004b: 342). Soon other cities were following suit, and by the 2005 general election nearly two million German voters were using these NEDAP machines to cast a vote (Der Speigel 2008). Reaction to the use of these electronic voting machines was generally very positive among voters, who found the machines to be easy to use, and among election administrators, who were able to reduce the numbers of polling stations and staff in each polling station (Commission on Electronic Voting 2004b: 343-5).

However, after the 2005 election, two voters brought a case before the German Constitutional Court after unsuccessfully raising a complaint with the Committee for the Scrutiny of Elections. The case argued that the use of electronic voting machines was unconstitutional and that it was possible to hack the voting machines; therefore, the results of 2005 election could not be trusted.

In a ruling that was a surprise to many, the German Constitutional Court upheld the first argument that the use of the NEDAP voting machines was unconstitutional (Federal Constitutional Court 2009). Many have misinterpreted or misquoted this ruling by the Constitutional Court to mean that the use of the electronic voting machine *per se* is unconstitutional in Germany. This is not the case. The findings of the Court are far more nuanced than this and in no way rule out the use of electronic voting machines.

The Court noted that under the constitution elections are required to be public in nature and:

> *"…that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception… The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of*

[100] See http://www.english.umic.pt/index.php?option=com_content&task=view&id=3113&Itemid=448#paraguay [last accessed 4 November].

[101] See the series of agreements between the two electoral management bodies at, http://www.tse.gov.br/internet/ingles/mundo/convenios_paraguai.htm [last accessed 4 November 2011].

[102] Electoral Court of Justice Resolution No. 12/2008 TSJE, at http://www.tsje.gov.py/legislacion/resoluciones/2008/resoluciones-12_0.html [last accessed 4 November 2011].

> *the result can be examined reliably and without any specialist knowledge of the subject… The very wide-reaching effect of possible errors of the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections."* (Federal Constitutional Court 2009: para II)

Making it clear that the decision of the Court did not rule out the use of voting machines in principal, it stated that:

> *"The legislature is not prevented from using electronic voting machines in elections if the possibility of a reliable examination of correctness, which is constitutionally prescribed, is safeguarded. A complementary examination by the voter, by the electoral bodies or the general public is possible for example with electronic voting machines in which the votes are recorded in another way beside electronic storage."* (Federal Constitutional Court 2009: para II)

This decision by the German Constitutional Court effectively ended Germany's current use of electronic voting. Although the Court decision does not rule out electronic voting machines entirely, no further moves to adopt machines which meet the transparency requirements have been made.

Emerging Trends

The four cases reviewed in the previous section where the use of electronic voting was discontinued are not only interesting, but also instructive of some of the emerging trends we see in the use of electronic voting. This section outlines seven emerging trends, many of which are interlinked.

Electronic Voting Standards

Electronic voting machines may seem, or can certainly be designed, to feel very similar to paper balloting from a voter's perspective; they can be designed to even look like a paper ballot. Electronic voting machines, which may, however, from a voter's perspective look similar to paper balloting, operate in a fundamentally different way, and require completely different regulatory and operational framework to ensure that voting machines support sound democratic practices.

General electoral standards have solidified around a number of principles in the past 10-20 years.[103] However, the emergence of electronic voting and counting has challenged these standards in a number of ways, requiring the framework of standards to adapt and cope with the different ways in which elections are managed using these technologies. At the same time the voting and counting technologies have been, and still are, developing and providing new functionalities. The development of new voting and counting technologies and electoral standards to guide the use of these technologies are interlinked. In some cases the technology will drive the development of standards as these standards have to cope with new ways of administering elections using technology. But there is causality in the other direction also, with emerging election technology standards influencing the development of new technologies as suppliers try to find better ways of meeting these emerging standards.

[103] Such as fair elections, genuine elections, periodic elections, universal suffrage, equal suffrage, secret ballot and free elections (Goldsmith 2011: 17-18).

The important point to make is that this interplay between technology development and emerging standards is ongoing, and the framework of electronic voting standards is yet to fully emerge. Significant work has begun, especially with the Council of Europe's 2004 recommendation on Legal, Operational and Technical Standards for E-Voting (Council of Europe 2004). The Council of Europe has followed this with a number of other documents which seek to establish standards for e-voting (Caarls 2010, Council of Europe 2011a, Council of Europe 2011b). The OSCE, OAS and EU have all issued documents which can be seen as contributing to the emerging standards that electronic voting and counting are expected to meet (OSCE 2005, OSCE/ODIHR 2008b, OAS 2010, European Commission 2006). There are also examples of influential NGOs supporting democratic elections, such as the Carter Center, National Democratic Institute for International Affairs and the International Foundation for Electoral Systems, which have published documents contributing to the development of election technology standards (Carter Center 2007, Pran and Merloe 2007, Goldsmith 2011).

None of these documents have the same authority as the ICCPR, which is the basis for general international electoral standards. The ICCPR is a treaty and therefore binding on all signatories. The most authoritative of the electronic voting documents is the Council of Europe's 2004 Recommendation, but even this is only a recommendation, and therefore not legally binding and, in principle, only relevant for members of the Council of Europe. Despite the fact that the Council of Europe Recommendation is not binding, it has still been taken by a number of European countries as a benchmark for any implementation of electronic voting. Even beyond the Council of Europe members it is seen as important and is often referenced by non-member states.

Given the development of new standards since the introduction of electronic voting, it is to be expected that many of the early electronic voting machines were of a lower quality in terms of supporting democratic and electoral principles. The period since the introduction of electronic voting has seen a significant improvement in the quality of machines being used. As the voting technology field is rapidly changing, and standards for electronic voting are yet to fully emerge, we can expect that the field of electronic voting will continue to change quite rapidly.

Need to Review Legal and Regulatory Framework

The implementation of electronic voting may entail relatively little change for electors in their voting transactions in the polling station. However, from an election administration perspective the comprehensive implementation of electronic voting will require fundamental review and reform of legal and regulatory frameworks. This review will need to include the following aspects of the legal and regulatory framework:[104]

- Transparency mechanisms that need to be implemented through the election law in relation to the use of electronic voting technologies, including access to key components of the election administration process using these technologies for observers
- Security mechanisms and safeguards would need to be established in legislation to ensure the accuracy and integrity of elections using electronic voting technologies

[104] Taken from (Goldsmith 2011).

- Legal requirements for initial and periodic independent certification of electronic voting systems
- Institutions permitted to conduct this certification and the registration process and requirements for certifying institutions and consequences of non-certification of electronic voting technologies
- Status of an election if the mechanisms for producing an audit trail did not work (e.g. the printer did not work or the machine ran out of paper)
- Legal status of the electronic record of voting produced by an electronic voting machine compared to the audit trail record, and which record takes precedence in the event they are different
- Circumstances under which the audit trail should and could be counted: legal requirements for mandatory audits of electronic voting machines, the scale of such mandatory audits and mechanisms for selection of the voting machines to be audited.
- Consequences of the audit process finding differences in the results between the electronic results and the count of the audit trail, and which results shall be used
- Mechanisms for challenging results generated using electronic voting technologies and instances in which a challenge against the result will lead to a manual recount of the audit trail for the voting machine

Transparency and Trust

Transparency and trust are important in any electoral system, including traditional paper balloting. As the German Constitutional Court succinctly argued, manipulation or acts of electoral fraud are possible in conventional elections with paper ballots, but only with a very high risk of detection. Programming errors or deliberate manipulations of the electoral software can only be recognized with difficulty and have the potential to fundamentally alter a result and therefore require special precautions (Federal Constitutional Report 2009: para. II).

Even where the need for transparency (or protection of the public nature of elections as it is phrased in the German Constitution) is not constitutionally required, transparency is a vital tool for building and maintaining trust when using electronic voting. Given the inherent lack of transparency with electronic voting technologies, greater effort needs to be made to create transparency in the electronic voting process. We simply cannot see how voting machines work, whereas the paper ballot can be monitored from being placed in the ballot box to being counted and tabulated.

Failing to provide this transparency along with other mechanisms to demonstrate the proper functioning of the electronic voting system can have devastating consequences for the perceived legitimacy of a system, regardless of how accurate perceived concerns are. A failure to appreciate the need for transparency is certainly partly to blame for the eventual rejection of electronic voting in the Netherlands. The origins of the popular movement against electronic voting machines was rooted in the lack of response to requests for access to the source code and evaluation reports, and the lack of verifiability of the machines.

The issue of the verifiability of electronic voting machine has become critical to the issue of transparency and trust and was also a feature in Germany and Ireland’s rejection of electronic voting to varying degrees, although not central to the Irish example. This verifiability can be achieved through a number of mechanisms. A common way of achieving this transparency with electronic voting machines is through the use of an audit trail which can be verified by the voter. Other actions can include using an open source code, transparent testing and certification procedures, open audit processes, regular contact with stakeholders to discuss concerns about the use of voting machines, voter verified audit trails, randomly selected public recounts of audit trails, observation of opening and closing voting machines, mock elections to test the voting machines and making all system documentation available.

The need for a form of voter verified audit trail,[105] normally a paper trail, is one of the emerging standards for electronic voting. The acceptance of this new standard can be seen by the fact that the Indian Election Commission is in the process of adapting its voting machines to have a voter verified paper audit trail, largely in response to this emerging standard (Election Commission of India 2011).

The important point to note when it comes to transparency and trust in electoral systems, and especially in electronic voting, is that the trust of the electorate can be volatile. As was seen in the Netherlands, just because voters had accepted electronic voting for over a decade did not mean that opinion could not turn quickly and decisively against it in the absence of transparency and trust-building mechanisms. Once issues related to trust in the use of electronic voting machines developed, and were not mitigated by the EMB and government, they soon led to a reversal in public opinion, which was terminal for the use of voting machines.

Election management bodies have to take these issues of transparency and trust very seriously if they are to avoid such reversals of public support for electronic voting machines, and the potential write off of millions of Euros of voting machine equipment. In order to do this, many transparency and trust building mechanisms need to be in place.

Voting System Security

The security of electronic voting systems has become an increasingly important public issue. Early electronic voting systems were implemented with very few, if any, security mechanisms or checks and balances to ensure that they accurately recorded votes. The 2000 U.S. presidential election can be seen as a global turning point in terms of the scrutiny that technology-based electoral systems were subjected to. That election clearly showed that technology, even if it was a well-established, was fallible and that checks and balances were essential if voters and contestants were to trust the results generated by the technology; although technology was far from the only problem in that election. This realization showed itself across many aspects of electronic voting, including a much greater scrutiny of the physical security of electronic voting machines and investigations into the possibility of infiltrating the code, which runs voting and results systems to manipulate election results.

Electronic voting machines and results systems did not fare well under this scrutiny. Despite the denial of voting machines suppliers, and often election administrators, numerous security flaws were often

[105] This audit trail is normally a paper record of the voter's voting transaction which can be counted manually to verify that the audit trail and electronic result agree. The audit trail needs to be seen by the voter, so that they can alert polling staff in case it differs from the vote cast, in which case the accuracy of the voting machine would be in question.

found in voting machines. In the Netherlands, campaigners argued that it was easy to reprogram voting machines to, for example, play chess or to manipulate the election results. When the suppliers of the machines challenged this, the campaigners went ahead and reprogrammed one of the voting machines to do exactly that, playing chess against a reprogrammed voting machine (Gonggrijp and Hengeveld 2006).

The Election Commission of India claimed that because the instructions for their voting machine were burned into the circuit board, it was not possible to reprogram their machines. Ron Gonggrijp, who was involved in proving the insecurity of the Dutch voting machines, along with a number of other researchers took on this challenge of showing how secure the Indian voting machine was. They demonstrated that with little effort the Indian voting machines could be manipulated to change the results, avoiding this circuitry coding, and that this manipulation could be activated by mobile phone (Prasad et al 2010).

In the U.S., the debate on electronic voting machine security has been particularly intense, with many studies demonstrating how existing machines could be hacked in order to manipulate election results (Kohno et al 2004: 27, Feldman, Haldermann and Felton 2007, Bannet et al 2004: 32-37).[106] Concerns about the physical security of the Irish voting machine were also identified by the Commission on Electronic Voting (Commission on Electronic Voting 2006: Part 4).

It is clear that the issue of physical and logical security of voting machines and the possibility that they may be hacked to manipulate election results are concerns which are very salient for electoral stakeholders, as well as being incredibly important for the integrity of the elections. Voting machine suppliers and election administrators have had to increase the measures implemented to ensure that this security is achieved. One of the key ways in which this security issue has been mitigated, or proposed to be mitigated, is through the provision of a voter verified audit trail so the ultimate security measure is that it is easy to detect if a voting machine has been manipulated.

Role of Stakeholders in the Decision Process

As is clear from the above discussion on transparency and trust, electoral stakeholders need to support the use of electronic voting machines. In the absence of this support, the electoral process and the elected institutions may be seen as not representing the will of the people. This will undermine the very basis of legitimate government and run contrary to the basic democratic requirements of the ICCPR.

While the transparency and trust mechanisms outlined above will do much to keep public opinion on board[107], it is important that stakeholders are engaged from the beginning of the process, especially in the initial decision on whether to adopt electronic voting machines. The Irish example shows how important this is. There was little consultation with voters and political parties as the decision was taken to adopt voting machines after the 2002 pilots. In fact the Oireachtas Joint Committee on Environment and Local Government which took the decision in December 2003 received presentations from civil

[106] Also see http://www.zdnet.com/blog/government/the-scary-truth-about-voting-machine-hacking-risk-exclusive-video/10945?tag=nl.e589 [last accessed 3 November 2011].

[107] Although even these will fail if there are democratic flaws in the electronic voting machines or the way in which they are implemented.

society and the Labour Party (the opposition), which did not support the introduction of electronic voting machines until outstanding questions about security and integrity of the voting machines had been answered. The Government's decision to force through the adoption of voting machines using its majority on the Joint Committee was incredibly risky.

At this point, political opposition to electronic voting machines consolidated and the issue was raised at every possible opportunity in the lower house of parliament. Civil society advocacy also increased, and the two combined led to increasingly negative publicity. This forced the government to establish the Commission on Electronic Voting (McDermott 2010: 75-6), which ultimately decided that the NEDAP voting machines were not suitable for use without modification.

Ironically the process that the Commission on Electronic Voting initiated in conducting its work, with a comprehensive public consultation exercise, was exactly the kind of process that should have taken place earlier in the decision making process. McDermott argues that had this process of public consultation, transparent decision making and advice from independent experts been conducted by the Department of Environment while making the decision on adoption of electronic voting machines, then the end result would have been very different in Ireland (McDermott 2011: 77). It certainly would have identified, much earlier, the concerns that ultimately led to rejection of the electronic voting machines. This being the case, specifications for the voting machines could have been adapted to mitigate concerns before the machines were bought, or the decision taken not to adopt voting machines without buying them first.

The key point to recognize is that it is incredibly risky to proceed with implementing electronic voting machines in the absence of support from voters and political parties. This absence of support may ultimately fatally undermine the conduct of electronic voting, after a significant investment in the system. The absence of opposition should also not be taken as implicit support for voting machines; it may merely mean that public opinion has not turned its attention to the matter. Election management bodies and governments need to actively engage stakeholders to ensure they support the decision to adopt voting machines, and if not then to work with them to deal with their concerns to the extent possible or recognize that their concerns are legitimate.

In this respect, events in Paraguay are instructive. Here the Supreme Electoral Court of Justice, in response to growing mistrust of the electronic voting machines, surveyed political parties. When little support for voting machines was found, the Supreme Electoral Court of Justice decided to stop the use of voting machines rather than risk damaging the integrity of the electoral process beyond repair. Obviously Paraguay was more easily able to change this policy having only borrowed voting machines from Brazil rather than having spent a large amount of money in buying them. While this financial argument cannot be ignored, this should not be the driving force behind decisions on the use of voting machines. Voting machines must support overall electoral integrity, not undermine it. To do so key electoral stakeholders must support the use of voting machines.

Critical Role of Election Management Bodies

Electronic voting projects are incredibly complex and require very strong project management skills on the part of the EMB to implement them in an effective manner which helps to build trust in the electoral process. This will require that effective operational procedures are put in place for electronic voting.

Unfortunately EMBs are sometimes ill-equipped to deal with these complex project management issues and the expert IT skills that they require. In such situations vendors often fulfill, frequently in the interests of delivering the project successfully, some of these project management functions which should, in principle, be conducted by the EMB. This is a dangerous situation for the integrity of elections. The EMB, whether institutionally independent or part of the government, is the body legally empowered to conduct elections and to do so in an independent and impartial manner. Effectively contracting out the management of a central component of the electoral process undermines this independence. It also fundamentally changes the relationship between the supplier of the electronic voting machines and the EMB by shifting the balance of control away from the EMB and toward the supplier (Oostveen 2010, Theisen 2008).

In addition, the EMB will need to work proactively to maintain the trust that it has hopefully built through the initial consultations with stakeholders, through the transparency and trust building mechanisms it has put in place. During the process of implementing electronic voting many concerns and issues will be raised by stakeholders, some legitimate and others without foundation. Election management bodies need to be responsive to these concerns and deal with them when they arise. Failure to respond can lead to the public agenda being defined by these concerns even if there is no foundation to them. Once control of this public opinion agenda is lost it is difficult to regain control over it.

This lack of responsiveness to issues raised by political parties, civil society and voters is certainly part of the reason for the eventual rejection of electronic voting in Ireland and the Netherlands. Election management bodies need not only to be responsive, but proactive in providing information and maintaining trust on an ongoing basis.

The example of the Philippines is instructive in this regard. During their 2010 implementation of electronic counting nationwide for the parliamentary election, they had dedicated a Commissioner and permanent staff to monitor and respond to the public debate about the use of electronic counting technology. This responsiveness and general openness of information meant that even with concerted efforts by a small group of citizens and civil society to undermine the electoral process, the implementation of the new technology was still seen as largely successful.

Ongoing Technology Developments

As outlined in the discussion on emerging electronic voting standards, voting technology is still a rapidly developing field as voting machines try to adapt to emerging standards, such as the voter verified audit trail, and also find better ways of implementing existing processes. There is one technological development which is beginning to emerge which is particularly worthy of note, and no doubt an indication of the direction in which voting machines will develop in the future – the integration of biometric voter identification mechanisms into voting machines.

This development can be seen in Brazil, where a pilot project in the 2010 presidential election saw over 1.2 million voters trialing voting machines with fingerprint identification.[108] In May 2011, Venezuela also implemented voting machines with integrated fingerprint authentication.[109] This development has much to offer electronic voting. Voting machines currently need to be activated, either directly by the polling staff, or through an activation key (possibly a magnetic card) provided to the voter once their eligibility to vote has been determined by the polling staff. This provides the possibility for polling staff, if corrupt, to activate the voting machine without proper voter authentication and to "stuff" the electronic ballot box.

Biometric authentication, which is built into the voting machine, provides the possibility to remove this possibility for fraud, by matching the biometric data held for registered voters with that from the person trying to vote. This ensures that only legitimate voters can vote, and that each voter can only vote once.

While the integration of this technology into voting machines has much to offer, it is not a technological development that every country could adopt easily. It requires that biometric data is held for all registered voters, something that relatively few countries in the world actually have, or that the significant task of collecting this data is undertaken. There are also concerns when voter authentication and voting are combined on the same machine that the secrecy of the vote will be violated and the link between the voter and the vote cast will be maintained by the machine. While this is a concern that can be easily dealt with from a technical perspective, the perception of this link being maintained may be difficult to dispel amongst electoral stakeholders.

Nevertheless, it is likely that electronic voting technologies will increasingly develop in this way, integrating biometric identification systems. Developments in this area and the experiences of Brazil and Venezuela in trialing the technologies will be of great significance for all interested in implementing electronic voting.

[108] "Brazilian election biometrics have 93.5 percent success rate," at http://news.xinhuanet.com/english2010/world/2010-10/04/c_13541727.htm [last accessed 3 November 2011].

[109] "Venezuela looks to expand electronic voting," at http://embavenez-us.org/_sanfrancisco/index.php?pagina=news.php&nid=5459 [last accessed 3 November 2011].

References

Appel, A. W. (2006)“Ceci n’est pas une urne: On the Internet vote for the Assemblée des Français de l’étranger”, at www.cs.princeton.edu/~appel/papers/urne.pdf

Allen Consulting Group (2011) Evaluation of technology assisted voting provided at the New South Wales State General Election March 2011, at http://www.elections.nsw.gov.au/__data/assets/pdf_file/0004/93766/July_2011_Final_ACG_iVote_Report_ELE01-C_Final.pdf [last accessed January 16 2012]

Avgerou, C., Ganzaroli, A., Poulymenakou, A. and Reinhard, N. (2007) “ICT and Citizens’ Trust in Government: lessons from electronic voting in Brazil”, Proceedings of the 9th International Conference on Social Implications of Computers in Developing Countries, Sao Paulo, Brazil, May 2007, at http://www.ifipwg94.org.br/fullpapers/R0098-1.pdf [last accessed February 23, 2012]

Avgerou, C., Ganzaroli, A., Poulymenakou, A. and Reinhard, N. (2009) “Interpreting the trustworthiness of government mediated by information and communication technology: lessons from electronic voting in Brazil”, in Information technology for development, vol. 15 (2), pp. 133-148

Bannet, J., Price, D. W., Rudys, A., Singer, J. and Wallach, D. S. (2004) “Hack-a-Vote: Security Issue with Electronic Voting Systems,” in IEEE Security and Privacy, January/February 2004, pp. 32-37

Barrat-Esteve, J. (2010) “El voto electrónico ante intereses contradictorios: la razón comercial contra el principio democrático. A propósito de los compromisos comerciales de confidencialidad (CCC)”, Democracia digital, participación y voto electrónico, Valencia: CEPS, pp. 57-69

Barry, C. and Brightwell, I (2011) “Technology Assisted Voting: NSW State General Election 26 March 2011”, NSW Electoral Commission, at http://www.elections.nsw.gov.au/__data/assets/pdf_file/0009/96066/Parliamentary_Presentation_10_Nov_2011_v4.pdf [last accessed February 17, 2012]

Belanger, F. and Carter, L. “The Digital Divide and Internet Voting Acceptance”, The Fourth International Conference on Digital Society, 10-16 February 2010

Bochsler, D. (2010) “Can Internet Voting Increase Political Participation? Remote electronic voting and turnout in the Estonian 2007 parliamentary elections”, at http://www.eui.eu/Projects/EUDO-PublicOpinion/Documents/bochslere-voteeui2010.pdf [last accessed January 16, 2012]

Brennan, G. and Petit, P. (1990) “Unveiling the Vote,” British Journal of Political Science, 20(3), pp. 311-333

Buchstein, H. (2010) “Public Voting and Political Modernization: Different Views from the 19th Century,” p. 17-26, Scrutin secret et vote public, huis clos et débat ouvert, seminar / first draft, Paris: Collège de de France, www.college-de-france.fr/media/rat_soc/UPL31828_buchstein_scrutin.pdf [August 14 2011]

Caarls, S. (2010) E-voting Handbook: Key steps in the implementation of e-enabled elections, at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf [last accessed January 12, 2012]

Canton de Berne (2011) “Succés du vote électronique pilote”, at http://www.be.ch/portal/fr/index/mediencenter/medienmitteilungen/suche.meldungNeu.html/portal/fr/meldungen/archiv/archiv9/mm_9798 [last accessed January 11, 2012]

Carter Center (2007) Developing a Methodology for Observing Electronic Voting, see http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf [last accessed November 3, 2011]

Christensen, T. and Laegreid, P. (2003) Trust in Government – the Significance of Attitudes Towards Democracy, the Public Sector and Public Sector Reforms, at http://www.ub.uib.no/elpub/rokkan/N/N07-03.pdf [last accessed February 1, 2012]

CNIL (2009) 30e Rapport D'Activite 2009, at www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf

Commission on Electronic Voting (2004a) "Interim Report of the Commission on Electronic Voting on the Security, Accuracy and Testing of Chosen Electronic Voting System", at http://www.epractice.eu/files/media/media_812.pdf [last accessed November 3, 2011]

Commission on Electronic Voting (2004b) "First Report of the Commission on Electronic Voting on the Security, Accuracy and Testing of Chosen Electronic Voting System", at http://www.epractice.eu/files/media/media_799.pdf [last accessed November 3, 2011]

Commission on Electronic Voting (2006) "Second Report of the Commission on Electronic Voting on the Security, Accuracy and Testing of Chosen Electronic Voting System", at http://www.umic.pt/images/stories/publicacoes1/Part%200%20Index.pdf [last accessed November 3, 2011]

Corritore, C. L., Kracher, B. and Wiedenbeck, S. (2003) "On-line Trust: Concepts, Evolving Themes, a Model", in International Journal of Human-Computer Studies, vol. 58, p. 737-758

Council of Europe (2004) Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory Memorandum, at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Key_Documents/Rec percent282004 percent2911_Eng_Evoting_and_Expl_Memo_en.pdf [last accessed November 3, 2011]

Council of Europe (2011a) Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards, Strasbourg: Council of Europe, at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf [last accessed January 12, 2012]

Council of Europe (2011b) Guidelines transparency of e-enabled elections, Strasbourg: Council of Europe, at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting percent202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf [last accessed January 12, 2012]

Delvinia Interactive (2007) Understanding the Digital Voter Experience: The Delvinia Report on Internet Voting in the 2006 Town of Markham Municipal Election

Der Spiegel (2008) "Court to Examine Security of Electronic Voting", at http://www.spiegel.de/international/germany/0,1518,587001,00.html [last accessed November 3, 2011].

Dieter, I. (2003) "Dispelling the Myth of Election 2000: Did Nader Cost Gore the Election?," at http://www.cagreens.org/alameda/city/0803myth/myth.html [last accessed November 3, 2011]

Drechsler, Wolfgang (2004) “The Estonian E-Voting Laws Discourse: Paradigmatic Benchmarking for Central and Eastern Europe,” Occasional Papers in Public Administration and Public Policy, 5(2), at www.nispa.sk/files/publications/occassional/NISPAcee_Occas_2004-2.pdf [last accessed October 28, 2011]

EISA (2003) Principles for Election Management, Monitoring and Observation in the SADC Region, The Electoral Institute for Sustainable Democracy in Africa: Johannesburg, at http://www.eisa.org.za/PDF/pemmo.pdf [last accessed January 11, 2012]

Election Commission of India (2011) Press Note No. ECI/PN/44/2011, at http://eci.nic.in/eci_main1/current/PN20071011.pdf [last accessed November 3 2011]

Enguehard, C. (2009) “Transparence, élections et vote électronique”, Démocratie électronique, Journée d'études de l'Association Française de Droit Constitutionnel, Besançon: Centre de Recherches Juridiques / Université de Franche-Comté, at hal.archives-ouvertes.fr/docs/00/43/59/66/PDF/Enguehard_Besancon2009.pdf [last accessed December 23, 2011]

Estonian Supreme Court (2005) – Decision 3-4-1-13-05, 1 September 2005, at www.nc.ee/?id=381

European Commission (2006) Methodological Guide to Electoral Assistance, see http://ec.europa.eu/europeaid/multimedia/publications/documents/thematic/ec_methodological_guide_on_electoral_assistance_en.pdf [last accessed November 3, 2011]

Federal Constitutional Court (2009) Press Release no.19/2009 of 3 March 2009, at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html [last accessed November 3, 2011]

Feldman, A. J., Halderman, J. A. and Felton, E. W. (2007) “Security Analysis of the Diebold AccuVote-TS Voting Machine,” in Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT’07)

Fuglerud, K. S., Halbach, T., Dale, Ø., Solheim, I. and Schultz, T. (2009) “Accessibility and usability evaluation of E-vote prototypes”, Norwegian Computing Centre, at www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf [last accessed January 6, 2012]

Goldsmith, B. (2011) Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies, Washington DC: IFES, www.ifes.org/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf [last accessed December 24, 2011]

Gonngrijp, R. and Hengeveld, W-J (2006) “Nedap/Groenendaal ES3B Voting Computer: a security analysis,” at http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf [last accessed November 3, 2011]

Goodwin-Gill, G. S. (2006) Free and Fair Election (Second Edition), Inter-parliamentary Union: Geneva, at www.ipu.org/pdf/publications/free&fair06-e.pdf [last accessed November 12, 2011]

Harris, B. (2004) Black Box Voting (Plan Nine Pub)

International IDEA (2002) International Electoral Standards: Guidelines for reviewing the legal framework of elections, International IDEA: Stockholm

Jacobs, B. and Pieters, W. (2009) “Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment,” in Proceedings of FOSAD'2008, at http://dare.ubn.kun.nl/bitstream/2066/75763/1/75763.pdf [last accessed January 12, 2012]

Jones, D. (2009) “Some Problems with End-to-End Voting”, End-to-End Voting Systems Workshop, Washington DC: National Institute for Standards and Technology (NIST), at www.divms.uiowa.edu/~jones/voting/E2E2009.pdf [last accessed December 23, 2011]

Jones, D. (2007) “The Impact of Technology on Election Observation”, VoComp, Portland: VoComp, at www.divms.uiowa.edu/~jones/voting/vocomp07.pdf [last accessed December 23, 2011]

Jones, D. (2003) “A Brief History of Voting”, at http://www.divms.uiowa.edu/~jones/voting/pictures/#dre [last accessed on January 12 2012]

Kohno, T., Stubblefield, A., Rubin, A. and Wallach, D. (2004) “Analysis of an Electronic Voting System”, IEEE Symposium on Security and Privacy, Washington DC: IEEE Computer Society Press, at avirubin.com/vote.pdf [last accessed on December 24 2011]

Kitteringham, K., Brouwer, A. and Tecsa, T. (2010) “Markham’s Online Voting Experience”, Municipal I-Voting Learning Summit, December 15 2010

Lang, B. (2006) “Rapport sur l'usage du vote électronique par l'Internet pour les élections à l’Assemblée des Français de l'Étranger de juin 2006”, at http://bat8.inria.fr/~lang/ecrits/liste/evote-internet-2006.html

Lewis, J. D. and Weigert, A. (1985) “Trust as a Social Reality”, in Social Forces, vol, 63:4, p. 967-985

Madise, Ü. and Vinkel, P. (no date) “ICT, I-voting and other e-services in Estonia”

Madisse, Ü. and Vinkel, P. (2010) “TIC, votacions per internet i altres serveis electrònics a Estònia,” Eines, p.62, at www.irla.cat/documents/eines-12-web.pdf [last accessed June 15, 2011]

McDermott, R. “Ireland: A Decade of Electronic Voting” in Yard, M. (ed.) (2010) Direct Democracy: Progress and Pitfalls of Election Technology, IFES: Washington DC

Mebane, W. R. Jr. (2004) “The Wrong Man is President! Overvotes in the 2000 Presidential Election in Florida,” in Symposium, vol. 2, no. 3, pp. 525-535

Ministry of Local Government and Regional Development (2011) Project mandate for e-vote 2011-project

Ministry of Local Government and Regional Development (2009) E-vote 2011: Accessibility and Usability Requirements, at http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/Accessibility_and_Usability_Requirements.pdf [last accessed January 11, 2012]

Ministry of Local Government and Regional Development (2006) Report: Electronic Voting – Challenges and Opportunities, at http://www.umic.pt/images/stories/publicacoes1/evalg_rapport_engelsk.pdf [last accessed January 6, 2012]

NIST (2009) Voluntary Voting System Guidelines (Drafts) Version 1.1, at http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf [last accessed November 13, 2011]

Nist (2009) End-to-End Voting Systems Workshop, Washington DC: National Institute for Standards and Technology (NIST), iavoss.org/mirror/e2evoting/ [lat accessed December 25, 2011]

Norden, L., Burstein, A., Hall, J. L. and Chen, M. (2007) Post Election Audits: Restoring Trust in Elections, New York: Brennan Center for Justice / Samuelson Law, Technology & Public Policy Clinic, www.brennancenter.org/page/-/d/download_file_50227.pdf [last accessed October 29, 2011]

OAS (2010) Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions, General Secretariat of the Organization of American States (GS/OAS), see *www.oas.org/es/sap/docs/Technology_percent20English-FINAL-4-27-10.pdf* [last accessed November 3, 2011]

Oostveen, A-M. (2010) "Outsourcing Democracy: Losing Control of E-Voting in the Netherlands," in Policy and Internet, vol.2, issue 4, article 8

OSCE (2005) Challenges of Election Technologies and Procedures: Final Report, Supplementary Human Dimension Meeting, PC.SHDM.GAL/5/05

OSCE/ODIHR (2011) "Estonia Parliamentary Elections 6 March 2011: OSCE/ODIHR Election Assessment Mission Report", Warsaw: OSCE/ODIHR, at www.osce.org/odihr/77557 [last accessed October 29, 2011]

OSCE/ODIHR (2008) "Swiss Confederation – Federal Elections 221 October 2007: OSCE/ODIHR Election Assessment Mission Report", Warsaw: OSCE/ODIHR, at http://www.osce.org/odihr/elections/switzerland/31390 [last accessed January 11, 2012]

OSCE/ODIHR (2008b) OSCE/ODIHR Discussion Paper in Preparation of Guidelines for the Observation of Electronic Elections, ODIHR.GAL/73/08

OSCE/ODIHR (2007) "Republic of Estonia Parliamentary Elections 4 March 2007: OSCE/ODIHR Election Assessment Mission Report", Warsaw: OSCE/ODIHR, at www.osce.org/odihr/elections/estonia/25925 [last accessed December 24, 2011]

OSCE/ODIHR (2006) "The Netherlands: Parliamentary Elections 22 November 2006: OSCE/ODIHR Election Assessment Mission Report", Warsaw: OSCE/ODIHR, at www.osce.org/odihr/elections/netherlands/24322 [last accessed December 24, 2011]

OVF (2011) The Power to MOVE, Arlington: Overseas Vote Foundation (OVF), at www.overseasvotefoundation.org/initiatives-Power-to-MOVE [last accessed November 1, 2011]

Pellegrini, F. (2006) "Rapport d'observations", at www.ordinateurs-de-vote.org/IMG/pdf/rapport_pellegrini.pdf

Pieters, W. (2006) "What proof do we prefer? Variants of verifiability in voting", Workshop on Electronic Voting and E-government in the UK, 27-28 February 2006, UK: Edinburgh at http://doc.utwente.nl/65114/1/Verifiability.pdf [last accessed November 20, 2011]

Pieters, W. and Becker, M. J. (2005) "Ethics of E-voting: An essay on requirements and values in Internet elections"

Pran, V. and Merloe, P. (2007) Monitoring Electronic Technologies in Electoral Processes: An NDI Guide for Political Parties and Civic Organizations, National Democratic Institute for International Affairs, see http://www.ndi.org/files/2267_elections_manuals_monitoringtech-preface_0.pdf [last accessed November 3, 2011]

Prasad, H. K., Haldermann, J. A., Gonggrijp, R. Wolchok, S., Wustrow, E., Kankipati, A., Sakhamuri, S. K. and Yagati, V. (2010) "Security Analysis of India's Electronic Voting Machines", at http://indiaevm.org/evm_tr2010-jul29.pdf [last accessed January 12, 2012]

Quesenbery, W. (2008) Connecting Usability and Accessibility in Elections, EAC Usability and Accessibility Roundtable, 27 March 2008, at www.upassoc.org/civiclife/voting/documents/usability_accessibility_eac_roundtable.pdf [last accessed January 11, 2012]

Ribeiro de Souza (no date) "Parties and Electoral Campaign Financing in Brazil: A Review of Legislation", at http://paperroom.ipsa.org/papers/paper_2137.pdf [last accessed February 22, 2012]

Rikken, Kristopher (2011) "Tallinn Looks to Disallow E-Voting at Local Elections", Estonian Public Broadcasting (ERR) at news.err.ee/Politics/42804d99-1344-47e7-832b-22a859470fd6 [last accessed January 11, 2012]

Scytl (2005) "Pnyx.core: The Key to Enabling Reliable Electronic Elections", Barcelona: Scytl Secure Electronic Voting, www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf [lat accessed December 23, 2011]

Seingry, G-F., (2008) "10 Proposals to Improve Voter Turnout for French Overseas Elections", at http://www.francais-du-monde.org/wp-content/uploads/2008/10/2008-10-propositionsrev.pdf [last accessed January 16, 2012]

Simons, B. (2011) "Report on the Estonian Internet Voting System", *Verified Voting Blog*, blog.verifiedvoting.org/2011/09/03/1435 [last accessed January 11, 2012]

Spycher, O., Volkamer, M. and Koenig, R. (2011) "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting"

Tarvainen, T. (2008) "Salassapitosopimuksen anatomia", Helsinki: Electronic Frontier Finland (EFFI), at www.effi.org/blog/2008-03-20-Tapani-Tarvainen.html [last accessed November 8, 2011]

Tennant, N. E. (2011) Legislative Report: West Virginia Uniformed Services and Overseas Citizen Online Voting Pilot Project, at http://www.sos.wv.gov/news/topics/elections-candidates/Documents/Report%20Final%202010%20General%20Election.pdf [last accessed January 16, 2012]

Theisen, E. (2008) "Vendors are Undermining the Structure of U.S. Elections," at http://www.votersunite.org/info/ReclaimElections.pdf [last accessed November 3, 2011]

Tjøstheim, I. (2011) "The use and challenge with everyday technology among visually impaired in Norway 2010", 26 September 2011, available at http://publications.nr.no/NR_note_6_2011_VI_survey_on_everyday_technologies_.pdf [last accessed January 11, 2012]

Tjøstheim, I. and Fuglerud, K. S. (2011) "Easy E-voting?," at http://www.forskning.no/artikler/2011/september/298728 [last accessed January 11, 2012]

Trechsel, Alexander H. (2011) "Internet Voting in Estonia: A Comparative Analysis of Four Elections since 2005," p.21 at www.vvk.ee/public/dok/Trechsel_Tallinn_March_2011.pdf [last accessed October 30, 2011]

Trechsel, A. H. and Vassil, K. (2010) Internet Voting in Estonia: A Comparative Analysis of Four Elections since 2005, Council of Europe/European University Institute/European Union Democracy Observatory, www.vvk.ee/public/dok/Report_-_E-voting_in_Estonia_2005-2009.pdf [last accessed November 20, 2011]

United Nations (1994) Human Rights and Elections: A Handbook on the Legal, Technical and Human Rights Aspects of Elections, United Nations Centre for Human Rights: New York and Geneva, at http://www.ohchr.org/Documents/Publications/training2en.pdf [last accessed January 11, 2012]

U.S. Election Assistance Commission (2011), "Testing and Certification Technical Paper #2: A Survey of Internet Voting – September 2011," at http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf [last accessed November 3, 2011]

Vähä-Sipilä, A. (ed.) (2009) "A Report on the Finnish E-Voting Pilot", p. 4, Helsinki: Electronic Frontier Finland (EFFI), at winston.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf [last accessed November 8, 2011]

Venice Commission (2004) Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, Strasbourg: European Commission of Democracy Through Law, at www.venice.coe.int/docs/2004/CDL-AD percent282004 percent29012-e.asp [last accessed October 28, 2011]

Vollan, K. (2011) "Internal Independent Verification of the Internet Voting Trial 2011", Version 0-4, 30 November 2011

Wand, J. N. (2001) "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County Florida," in American Political Science Association, vol. 95, p. 793-810

Annexes

Annex 1 – Data Sheets: Unsupervised Internet Voting:[110]

- Australia – New South Wales
- Canada
- Estonia
- France
- The Netherlands
- Spain
- Switzerland-Geneva
- United Kingdom
- United States-West Virginia

[110] A datasheet on the Indian experiments with internet voting is not included as it has not yet been possible to find out sufficient information on these trials.

Data Sheet – Internet Voting
Australia – New South Wales

Introduction	Parliament requested the NSW Electoral Commissioner to investigate the feasibility of remote electronic voting for vision-impaired and other disabled persons, with the primary objective being to enable a secret vote for people who are blind or vision impaired. Following initial consultations and previous reports into accessibility of the voting process, it became apparent that a remote electronic voting system would be of benefit to a broader audience of stakeholders than the blind and vision impaired. As a consequence, the stakeholder group was defined as: • people who are blind or vision impaired (around 70,000 electors); • people with other disabilities (around 330,000 electors); and • people in remote locations (around 6,500 electors). An assessment of the numbers of stakeholders (around 400,000 electors) and potential take-up rates estimated that between 5,000 and 15,000 votes could be cast using a remote electronic voting system if it was introduced for the State General Election in 2011 (SGE 2011). Previous studies undertaken for the New South Wales Election Commission (NSWEC) indicated that a remote electronic voting system could be a cost-effective option of enabling a secret vote for people who are blind or vision impaired. A 2010 feasibility report supported this assessment and recommended that remote electronic voting was technically feasible and that such a system can be implemented for the limited stakeholder group in time for the SGE 2011. [taken from NSWEC (2010) – Report on the Feasibility of providing "iVote" Remote Electronic Voting System, at http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/84498/20100723_NSWEC_iVote_Feasibility_Report_.pdf] It is worth noting that the NSW example is not Australia's first experience with Internet voting. In 2007 a trial was implemented for selected armed forces personnel posted overseas to cast their ballots in federal elections through the Internet. A total of 1,511 armed forces personnel overseas used this trial voting channel. In 2009 the Joint Standing Committee on Electoral Matters recommended that these trials not be continued. This recommendation was due to high cost of Internet voting and an assessment that postal voting for overseas armed forces personnel was more reliable and imposed fewer burdens on personnel. In 2006 and 2010, the Victoria Election Commission also trialed Internet voting from kiosks, but on a small scale, with only 199 and 841 voters using the service in the respective elections.
Years of Use	2011
Type of Elections/Referenda	State Government Elections
Type and Status of the Internet Voting Option	Voting from PCs in uncontrolled environments. The legal basis for conducting Internet voting for elections is not limited in duration and therefore this should not be considered as a pilot. The current legislation for Parliamentary elections in NSW requires the use of iVote unless the Commissioner decides otherwise. At this time the Commissioner has not made any specific decisions about the continuing use of the iVote system as it requires government approval and additional funding. The Commissioner has stated publicly that he sees iVote in the mix of voting channel options in the future.
Brief Description of	Eligible voters who wished to use the Internet voting system for the NSW State General Elections were required to pre-register in order to do so. On registration, which was

Internet Voting System	conducted either by phone or online, the voter would register a 6 digit passcode of their choice. After registration, an 8 digit voter ID code is sent to their home address by mail. Voters need to enter both the 8 digit voter ID code and the 6 digit passcode in order to vote online. Voting was from any computer with access to the Internet or Phone, and once voting was completed the voter was provided with a receipt number that could be used to check that the vote was included in the count (but not confirm the value of the vote).
Eligible Voters	Optional. Target voters - voters with disabilities; voters with blindness or low vision; illiterate voters; voters outside New South Wales on Election Day (absentee voters); and voters who live 20 km or more from a polling place. Pre-registration for Internet voting was required.
Other Voting Channels Available	Telephone (PSTN using DTMF tones) option using the same Internet voting infrastructure and was also made available at the same time as Internet voting, as well as the existing options of polling station voting, postal voting and assisted early voting at some locations.
Period of Internet Voting	12 days until the day before election day.
Legal Basis for Internet Voting	The Parliamentary Electorates and Elections Further Amendments Act 2010, which requires the "Electoral Commissioner to conduct an investigation as soon as possible into the feasibility of providing Internet voting for vision-impaired and other disabled persons for elections under this Act and, if such Internet voting is feasible, to propose a detailed model of such Internet voting for adoption."
Internet Voting Usage	Of the 51,103 who pre-registered to use remote voting services, 44,605 cast a vote through the Internet and 2,259 by telephone.
Voter Identification Mechanisms	Voters identify themselves with the 8 digit code sent to them after registration as an Internet voter and the 6 digit PIN number the voter provided on registration.
Vote Verification Mechanisms	Once the vote is complete, the elector will receive a receipt number that can be used later to confirm that the vote went into the count.
Secrecy Protection Mechanisms	No special measures
Internet Voting System Provider	Everyone Counts provided core voting system
Intellectual Property Rights of the Internet System	The intellectual property rights for the "core voting system" were held by Everyone Counts. There were however many peripheral systems (i.e. the registration system) and associated documentation for which the NSWEC own the intellectual property rights.
Open/Closed Source Code	The source code for the "core system" is proprietary, but selected parts were available to NSWEC during testing and assessment phases of the project for code review. All other system code was owned by NSWEC and available for review internally. NSWEC did not provide code in an open source model due to security and intellectual property reasons.
System Testing and Certification Mechanisms	PricewaterhouseCoopers (PwC) was engaged by the NSW Electoral Commissioner to undertake an audit of the technology assisted voting application, iVote. It released pre and post election audit reports. An evaluation of the system was also done by The Allen Consulting Group after the election. All reports are on the NSWEC website

	(http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports).
Voting and Results Audit Mechanisms	The NSW Electoral Commission appointed an independent auditor to report to the Electoral Commissioner at least 7 days before voting commences and again within 60 days of the return of the writs. The Auditor determined whether test votes cast in accordance with these approved procedures were accurately reflected in the corresponding test ballot papers.
Transparency Mechanisms	Scrutineers were present to observe the sealing and unsealing and printing of iVote ballots; election officials with electronic keys opened the electronic ballot box.
Court Cases Against the Use of Internet Voting	The number of complaints about iVote were very small and mainly related to one of the following areas; a) Could not access the system because the technology being used by voter was not compatible or voter error b) Did not receive credential information c) Thought they had voted, but did not complete the process properly due to either voter or system issues The number of written complaints was approximately 10 from the 46,864 electors who voted using the system.
Key Reports/ Documents	http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports

Data Sheet – Internet Voting
Canada

Introduction	To date, there have been many instances where Internet voting has been used in elections in Canada – all of which have been at the municipal level. The first experiences with Internet voting occurred in 2003 in over 10 municipalities in Ontario – the largest being in the town of Markham (population nearly 300,000). The number of municipalities using Internet voting for elections in Ontario has grown and, in 2010, over 40 municipalities in Ontario used online voting in conducting their general election. In addition, in 2008, Halifax and three other Nova Scotia municipalities incorporated Internet voting as an alternative voting method. In 2009, Halifax implemented an expansion of that approach in a by-election. This data sheet will focus on the longest running example of Internet use in Canada – Markham. The driving force for implementing Internet voting was identified as the desire to enhance service excellence, as well as the belief that Internet and telephone voting are a natural extension of election services. As the municipal participants expressed it, introducing Internet voting is a means of taking leadership with respect to electronic service delivery and is also an important step in enhancing convenience and accessibility for electors. Not only has it allowed the municipalities to better adapt to meet the changing lifestyles of electors, it has also improved accessibility, especially for special populations of electors such as university students, retirees and persons with disabilities. The Town of Markham, Canada's high-tech capital, became the first major municipality in Canada to pilot the implementation of Internet voting for the 2003 municipal election. This pilot was intended to evaluate the potential for increased voter turnout by improving accessibility and efficiency of the voting process and to prompt exploration of issues raised by the technology. In November 2006, the Town of Markham offered Internet voting as an option for advance poll voting for the second election in a row. Once again, the results were a success and provided further evidence that Internet voting is a viable addition to the electoral process, which meets the changing needs of both municipalities and voters. On a national level, the Canada Elections Act includes a provision authorizing research regarding alternative voting methods and the potential to study and/or test electronic voting processes (Canada Elections Act, s. 18.1). Deputy Chief Electoral Officer, Rennie Molnar, recently explained that Elections Canada is examining Internet voting as part of an ongoing strategic objective to continue to increase accessibility to the electoral process. Mr. Molnar pointed out that an amendment to the Canada Elections Act in 2000 permits Elections Canada to conduct an electronic voting experiment with the prior approval of Parliament. The target group selected to test on-line voting could include electors with disabilities or limited mobility, overseas electors or electors who are away from their electoral district on polling days.
Years of Use	2003, 2006 and 2010
Type of Elections/ Referenda	Local government elections
Type and Status of the Internet Voting Option	Remote voting from PCs in unsupervised environments. Local authorities are allowed to use alternative voting systems through the passage of local by-laws for local government elections. A number of local authorities, including Markham, have exercised this option over the past decade to allow Internet voting as an alternative to other existing means of voting. As this is an ongoing use of Internet voting for local elections this should not be considered as a pilot.

Brief Description of Internet Voting System	Markham – pre-registration required. All voters receive an online registration package. When registering voters select a unique security question, whose response is required before voting can take place. Online registration also removes the voters name from the paper ballot voter list, who cannot then cast a ballot at the polling station. Registered voters were sent a PIN number by post which together with their security question is used to authenticate them online to vote.
Eligible Voters	All registered voters are able to use Internet voting if they wished to do so, although pre-registration for Internet voting is required.
Other Voting Channels Available	Voting in polling stations, early postal voting
Period of Internet Voting	In 2003, a five day early voting period. In 2006 and 20ten, a six day early voting period
Legal Basis for Internet Voting	At the local level in Canada, municipalities are able to pass by-laws that allow for the use of alternative voting methods. If there is any conflict between a by-law and the existing legislation, the by-law supersedes anything contradictory in the legislation. At the federal or provincial levels, since there is no by-law option, the government must grant the chief electoral officers the power to try different forms or methods of voting. At the federal level, for instance, section 18.1 of the *Canada Elections Act* (introduced by Bill C-2 and assented on May 31, 2000) authorizes the Chief Electoral Officer to carry out studies and tests on alternative voting means, including electronic voting processes. However, prior to the implementation of such a process in an official vote, it is required that the proposed method or system be approved by House of Commons and Senate committees.
Internet Voting Usage	2003 – 7,210 online voters 2006 – 10,639 online voters 2010 – 10,597 Internet voters out of 65,927 total votes cast (16% votes cast by the Internet)
Voter Identification Mechanisms	A two-step Internet voting process was implemented to help authenticate voters. Step one required eligible voters to register online and establish their own unique password. Step two involved the receipt of a personal identification number (PIN) in the mail. Both the password and PIN were mandatory fields of data required to cast a vote online.
Vote Verification Mechanisms	None
Secrecy Protection Mechanisms	No special measures
Internet Voting System Provider	ES&S (2003 and 2006), ES&A and Intelivote Systems Inc. (2010)
Intellectual Property Rights of the Internet System	The application itself is proprietary property of ISI Intelivote Systems, Inc.

Open/ Closed Source Code	The vendor agreed to provide access to the source code as part of the audit. The exception to that was the client side coding which was available for the auditors by looking at the source code of the web pages.
System Testing and Certification Mechanisms	Functional and system testing was performed by the vendor. Markham performed extensive User Acceptance testing that included elements of Functional, System and Security testing
Voting and Results Audit Mechanisms	An auditor module was a component of the application used in the 2010 election. This module allowed the auditor to cast "audit" (marked) votes prior to, during and post elections attesting the correct assignment of the vote to the proper candidate The auditor module allowed the auditor to see before and after the casting the vote and thus attesting that the vote is counted.
Transparency Mechanisms	Markham saw the Auditor Module as having addressed this concern by allowing the auditor to cast audit votes prior to, during, and post elections.
Court Cases Against the Use of Internet Voting	None.
Key Reports/ Documents	http://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote&document=summary&lang=e Kitteringham, K., Brouwer, A. And Tesca, T. (2010) "Markham's Online Voting Experience", paper presented at Municipal I-Voting Learning Summit, December 2010 Delvinia (2006) "The Delvinia Report on Internet Voting in the 2006 Town of Markham Municipal Election"

Data Sheet – Internet Voting
Estonia

Introduction	Estonian Internet voting should be considered a milestone in an overall e-strategy. It is also closely linked to the distribution of ID cards that include cryptographic protocols to ensure remote authentication and digital signature. The successful deployment of these ID cards has been essential for the Internet voting project because it eases the significant challenge of authenticating the voter. Estonia was the first country to use Internet voting nationwide for political elections (not *referenda*). The first three elections were carried out without major criticisms and with a growing participation of Internet votes. The last election saw a significant increase in usage and a parliamentary committee has been subsequently created aimed at evaluating the system and suggesting potential improvements.
Years of Use	2005, 2007, 2009, 2011
Type of Elections/Referenda	2005 (local), 2007 (parliamentary), 2009 (European and local), 2011 (parliamentary)
Type and Status of the Internet Voting Option	Internet voting from PCs in unsupervised environments. Use of Internet voting is an ongoing option for voters at all European, Parliamentary and local elections.
Key features of the internet voting system	Besides some patterns usually used in Internet voting consultations, this case included some other specific features: (i) authentication procedures and (ii) measures foreseen to protect the freedom of the vote. Estonian citizens have an electronic ID card that is used for several transactions and therefore access to the Internet voting platform is conceived as another usual e-process within the governmental sphere. It is not necessary to include *ad-hoc* authentication methods. Voting from non-supervised environments entails serious concerns regarding the secrecy of the vote and the freedom to vote itself. While the anonymity of the vote can be guaranteed using PKI, the privacy of the voting act cannot. But according to the decision of the Estonian Supreme Court shall be compensated using a "virtual voting booth", i.e. the possibility for repeat voting and the replacement of an Internet vote with another Internet vote or with a paper-ballot during advance voting days. The freedom to vote is guaranteed by the same means.
Eligible Voters	No restriction is foreseen regarding eligible voters; no pre-registration is required, although voters should have a valid ID (ID card, digital ID or mobile ID).
Other Voting Channels Available	Paper ballot on Election Day and in the advance period, postal vote and voting in embassies for Estonians living abroad, at-home voting and voting from ships.
Period of Internet Voting	Internet votes may be cast during 7 days, from 10th day until 4th day before the election day.
Legal Basis for Internet Voting	www.vvk.ee/general-info/legal-acts There is one Electoral Act for each type of election; they contain certain data regarding Internet voting, but they are not detailed and not comprehensive regulations. There is also a Decree issued by the National Electoral Committee (NEC) and internal operational guidelines.

<table>
<tr><td><b>Internet Voting Usage</b></td><td>www.vvk.ee/voting-methods-in-estonia/engindex/statistics
Internet voting statistics for the 2005, 2007, 2009 and 2011 elections
<table>
<tr><th></th><th>2005 LE</th><th>2007 PE</th><th>2009 EPE</th><th>2009 LE</th><th>2011PE</th></tr>
<tr><td>I-votes counted</td><td>9,287</td><td>30,243</td><td>58,614</td><td>104,313</td><td>140,764</td></tr>
<tr><td>Number of all votes counted</td><td>502,504</td><td>555,463</td><td>399,181</td><td>662,813</td><td>580,264</td></tr>
<tr><td>I-votes among all votes</td><td>1.9%</td><td>5.5%</td><td>14.7 %</td><td>15.8%</td><td>24.3%</td></tr>
<tr><td>I-votes among total advance votes given</td><td>7.2%</td><td>17.6%</td><td>45.4%</td><td>44%</td><td>56.4%</td></tr>
<tr><td>I-votes cast abroad (51 countries in 2007, 66 in EPE and 88 in LE 2009)</td><td>n.a</td><td>2%
51 states</td><td>3%
66 states</td><td>2.8%*
88 states</td><td>3.9%
105 states</td></tr>
<tr><td colspan="6">* only temporary abroad</td></tr>
</table>
</td></tr>
<tr><td><b>Voter Identification Mechanisms</b></td><td>(i) ID card
(ii) digital ID card (without picture, signature and other ID features)
(iii) mobile ID</td></tr>
<tr><td><b>Vote Verification Mechanisms</b></td><td>Neither return codes nor end-to-end measures are foreseen.</td></tr>
<tr><td><b>Secrecy Protection Mechanisms</b></td><td>Beyond the cryptographic measures, the system also allows multiple voting and paper-ballots during the advance period. Paper ballots supersede Internet votes.</td></tr>
<tr><td><b>Internet Voting System Provider</b></td><td><i>Cybernetica</i></td></tr>
<tr><td><b>Intellectual Property Rights of the Internet System</b></td><td>The system owner is the National Electoral Committee.</td></tr>
<tr><td><b>Open/Closed Source Code</b></td><td>Observers are allowed to read the source code after signing a Non-disclosure Agreement (NDA).</td></tr>
<tr><td><b>System Testing and Certification Mechanisms</b></td><td>(i) formal certification is not foreseen
(ii) IT auditors (e.g. KPMG Baltic, PWC) conduct an audit only checking the compliance with the operation manual
(iii) tests are conducted by the project manager, by the <i>Cyber Defense League</i> and by a computer expert hired by NEC
(iv) public demo elections</td></tr>
<tr><td><b>Voting and Results Audit Mechanisms</b></td><td>No specific voting and results audit mechanisms.</td></tr>
</table>

Transparency Mechanisms	Training sessions for observers. Some reports are kept secret while others are informal or only delivered to observers, not the public in general.
Court Cases Against the Use of Internet Voting	(i) Supreme Court (3-4-1-13-05, 1.09.2005); (ii) in June 2011, the Tallinn City Council filed a lawsuit against different voting channels.
References	http://www.vvk.ee/voting-methods-in-estonia/engindex OSCE Election Observation Reports - http://www.osce.org/odihr/elections/estonia Madise, U. and Vinkel, P. – ICT, I-Voting and Other E-Service in Estonia

Data Sheet – Internet Voting
France

Introduction	France was one of the first countries to experiment with internet voting. In 2001, an Internet voting experiment took place in Voisins-le-Bretonneux using a kiosk, which was set up in the polling station. Further experimental piloting took place in Vandoeuvre-les-Nancy in the 2002 Presidential Elections. The 2002 local elections in Issy-les-Moulineaux also had experimental piloting. However, these pilots were mock elections with voters casting a paper ballot and having the opportunity to trial an Internet vote, which did not count towards the election. France is better known for its use of Internet voting for the election of its Assembly of French citizens living abroad. It is this more recent use of Internet voting, which is the focus of this data sheet. The French approach to Internet voting for expatriates has evolved from a simple transposition of the postal voting mechanisms to the Internet (not by accident do the first legal texts on the topic mention “voting by electronic post” - “vote par correspondance électronique”) towards one which acknowledges the many differences from postal voting. After having contracted a different company to run each single election of the Assembly of French citizens living abroad, the government bought a permanent Scytl license, which allows for an unlimited number of elections. This may lead to a so-far non-existing long-term approach to Internet voting. For this to happen, a process of “industrialization” of Internet voting should take place. For the time being, however, no permanent system is foreseen and a hosting solution must be found for each election.
Years of Use	2003, 2006 and 2009.
Type of Elections/Referenda	Internet voting is used for the election of the Assembly of French citizens living abroad. This consultative assembly of 155 members elects 12 senators who represent French expatriates (indirect election) in the Upper House.
Type and Status of the Internet Voting Option	Internet voting is conducted from computers in unsupervised environments. Internet voting is limited to French expatriates. In 2012, thanks to a constitutional amendment adopted in July 2011, the 1.5 million French expatriates will for the first time be able to participate in parliamentary elections to elect 11 representatives in the lower chamber of the parliament. This election will be direct, unlike the designation of the Senators representing French expatriates.
Brief Description of Internet Voting System	In 2003, 2006 and 2009, France has contracted a service provider to run the election of the Assembly of French citizens living abroad. While the systems are required to abide by the recommendations made by the CNIL (Commission nationale informatique et liberté, or National Commission on IT and Freedom), which provides guidelines for Internet voting systems and updates them over the years, little is known about them beyond the CNIL requirements. In all three elections so far, an electoral bureau made of party representatives, representatives of the French living abroad, and the various Ministries involved (interior and foreign affairs) supervised the vote to guarantee the proper and fair functioning of the system. This commission was given the encryption keys of the ballot box by the system’s operator and opened the ballot box with these keys at the end of the voting period.

	In 2003, a system with double envelopes was used. In 2006, the electronic roll and the electronic ballot box were stored on two different computers. An applet was downloaded in the voter's computer. The applet ensured the validity of the vote (preventing over votes, for instance) and encrypted the ballot with the public key. A second validity check was performed on the ballot when it reached the server storing the votes. In 2009, the Pnyx system from Scytl was used.
Eligible Voters	In 2003, the 50,000 registered French citizens living in North America (Canada and USA) could vote online. In 2006, the 525,000 French expatriates living in Asia, Europe and the Middle East could vote online. They had to register with their consulate prior to the ballot to be able to vote online. In 2009, the 340,000 registered French citizens living in Africa, North and Latin America could vote online. They had to register online with their consulate prior to the ballot to be able to vote online.
Other Voting Channels Available	Advance postal voting and polling stations on ballot day in embassies and consulates.
Period of Internet Voting	From the 19th to 31st May 2003. The polling stations opened on June the 1st. From the 6th to the 12th June 2006. The polling stations opened on June the 18th. From the 20th May to the 4th of June 2009. The polling stations opened on June the 7th.
Legal Basis for Internet Voting	The original law is that of 28 March 2003, authorizing postal and Internet voting for the election of the Assembly of French citizens living abroad. It is accompanied every three years by a decree that regulates the role and the composition of the electoral bureau, the procedures to be followed for Internet voting and the voters' identification method. This decree also requires the ballot organizers to comply with the latest sets of guidelines by the CNIL. These guidelines are also promulgated by a decree and are part of the legal basis for Internet voting. 2003: Decree 2003-396 of April the 29th 2003. 2006: Decree 2006-285 and government order of April the 6th 2006. 2009: Decree 2009-525 of May the 11th 2009. This decree foresaw exceptions to the possibility to vote online for the French living in countries that do not accept encryption of data transfer over the Internet.
Internet Voting Usage	In 2003, there were 50,000 eligible voters in Northern America. The total turnout reached 14.47%; 60.60% of all cast votes were cast online. In 1997, prior to the introduction of Internet voting, the turnout had reached 15.10%. 2006: there were 525,000 potential eligible voters. 28,000 registered to vote online and 10,201 actually cast an online vote. The total turnout was 14% and the share of online votes was also 14%. In 2009, there were 340,000 eligible voters. 64,831 cast a vote (19%), 6,091 of them did it online. The share of online ballots reached 9% of all cast ballots.
Voter Identification Mechanisms	2003: No information available. 2006: Voters identified themselves with an identifier and a secret code received by

	post and a password received by email. The voter identifies himself on the voting web site with the identifier and the password and validates his vote with the secret code. 2009: Voters identified themselves with the consular ID numbers and their personal password. These were automatically generated after the voters connected to the web site of the Association of French Citizens Abroad (AFE) to register to vote online.
Vote Verification Mechanisms	2003: No data available. 2006 and 2009: The voters received a receipt attesting that their vote had been received by the voting server.
Secrecy Protection Mechanisms	None.
Internet Voting System Provider	2003: Election Europe, formerly known as Election.com. 2006: EDAS provided the solution and Experian ran the election. 2009: Scytl provided the solution and Athos Origin hosted the election.
Intellectual Property Rights of the Internet System	In all three cases, the intellectual property belonged to the vendor.
Open/Closed Source Code	2003, 2006 and 2009: closed. In 2006 and 2009, the legal provisions stipulated that the expert should receive the source code. In 2006, this was denied by the vendor.
System Testing and Certification Mechanisms	The 2006 and 2009 decree mandate that an independent expert audit the confidentiality, security, accuracy and ballot operation control guarantees, before the opening of the ballot. The expert shall have sole access to the source code. He shall hand over his report to the ministry of foreign affairs and to the electoral commission. No publication was foreseen and no publication took place.
Voting and Results Audit Mechanisms	None
Transparency Mechanisms	None
Court Cases Against the Use of Internet Voting	None directly linked to Internet voting. The 2009 election in the constituency of Washington (USA) was annulled and repeated in 2010 after an unelected candidate claimed that the many problems encountered with postal voting meant that the outcome of the election in this constituency did not reflect accurately the voters' will. Yet irregularities in the exploitation of the system have been noted such as in 2006 the fact that the company Experian kept a copy of the ballot box encryption key while it should legally not have done so. In 2006 the expert noted the low number of Internet votes in some constituencies (only one person had requested to be allowed to vote online in Kabul, Skopje or Riga, for instance) and given the fact that the electoral bureau received the list of voters having voted online, the vote secrecy in these constituencies could not be guaranteed. Therefore, Internet voting from these countries was blocked before the end of the election period.
References	"Rapport d'observations" établi par François Pellegrini, 12th June 2006,

	www.ordinateurs-de-vote.org/IMG/pdf/rapport_pellegrini.pdf “Rapport sur l'usage du vote électronique par l'Internet pour les élections à l’Assemblée des Français de l'Étranger de juin 2006” by Bernard Lang, http://bat8.inria.fr/~lang/ecrits/liste/evote-internet-2006.html “Ceci n’est pas une urne: On the Internet vote for the Assemblée des Français de l’étranger” by Andrew W. Appel, www.cs.princeton.edu/~appel/papers/urne.pdf

Data Sheet – Internet Voting
The Netherlands

Introduction	The Rijnland Internet Election System (RIES) was developed for the Rijnland water board. Dutch water boards are regional government bodies in the Netherlands. There are 27 regional water authorities, all of which hold elections, operate independently, and levy their own taxes. The general administrative body is elected for a period of four years. The RIES was developed in a context in which postal voting was the norm. Hence certain standard aspects of elections like freedom of the vote have not been a prime consideration. After the 2006 national elections, the OSCE published its traditional Election Assessment Report, which contained the following remark: “The [OSCE] found broad consensus amongst both developers and critics of electronic voting that RIES would not be a suitable system for the possible expansion of Internet voting to the general population if this is to be considered.” The RIES Internet voting system was a collateral victim of the campaign of the “We do not trust voting computers” group targeting the use of electronic voting machines in the Netherlands, and had to be discarded while developments were under way for the 2008 parliamentary election. After electronic voting machines were banned in 2007 by a Ministry of Interior decree and a legal decision, the Ministry went on to ban Internet voting due to its alleged lack of security. RIES was the first Internet voting system to provide voters with a confirmation of their choice after the election thanks to its end-to-end auditability.
Years of Use	2004 and 2006
Type of Elections/ Referenda	The election of water board councils in 2004 and of the national parliament in 2006.
Type and status of the Internet Voting Option	Voting from PCs in unsupervised environments. RIES was considered as a voting system which could evolve into a broader Internet voting system. Internet voting using REIS has been discontinued since 2007.
Key features of the internet voting system	The RIES system departed from the “standards” of Internet voting systems in at least two ways: • The keys were centrally generated in a pseudorandom way, from a master key, and the key pairs were distributed to the voters. While normally, only the voter knows his private key, here the voter must trust that he is the only one knowing it. If a private key leaks, anyone knowing it can cast a vote on behalf of the voter to whom it belongs. Voters must also trust that no one keeps track of who gets which pair of keys, as this would breach ballot secrecy. The delivery of the key to the voters occurs through postal mail. After voting, voters should make sure that the key was destroyed. • Votes are stored unencrypted in the voting server. The main innovation brought by RIES lies in its end-to-end auditability. Before the elections, a pre-election reference table was published which contained all possible valid votes represented by key-less hashes together with a mapping to the corresponding candidates. During the election, the votes cast by legitimate voters build up a post-election table where the votes were represented by hashes made using the voters’ secret key. The outcome of the election was calculated by computing key-less hashes of each vote in the

	post-election table. If the vote is valid, its hash value can be found in the pre-election table and the chosen candidate can be determined. And since this hash is a key-less hash anyone can compute it, hence anyone can check the result of the elections. To this scope, at the end of the voting procedure, the voter received a “technical vote” and a control value (code). Each voter could verify whether his vote has been taken into account and how (which value) by looking at the table of preliminary or final results posted on the Internet. The security of the RIES system mainly depended on the use of administrative procedures and trust in these procedures.
Eligible Voters	For water boards elections: all residents of the water board district. For national elections: Dutch residents abroad who registered in advance (up to 4 weeks before election day).
Other Voting Channels Available	For water board elections and for national elections for Dutch residents abroad: advance postal voting.
Period of Internet Voting	I-votes could be cast during four days before election day.
Legal Basis for Internet Voting	The legal regulation of electronic voting (voting machines and Internet voting) in the Netherlands was complex. The Elections Act provides for the traditional method of paper balloting, whether in polling stations or by post. Voting by electronic machine was not regulated in primary legislation. The legal basis of such voting was confined to the Elections Decree of 1989, the Regulation on Approval of Voting Machines of 1997 and the Ministerial Circular on Security of Use and Storage of Voting Machines of 2006. The Online Voting Experiments Act provided for voting via the Internet. Its interim nature recognized the need for trial and cost effectiveness evaluation before any introduction nationwide. This regulation at the level of secondary legislation can be explained by the wish to allow flexibility in terms of facilitating amendment to keep abreast of technological advance. For the Dutch citizens abroad, a law was passed in 2003 to soften the existing regulations, notably the requirement of a signed affidavit joined to the postal vote. This enabled them to vote by Internet.
Internet Voting Usage	In 2004, about 120,000 votes (out of a potential of 2.2 million eligible voters) were cast with RIES for the election of the water boards of Rijnland and Dommel, in the course of two separate elections. Rijnland's previous election in 1999 was run by postal ballot. The overall turnout was in the order of 22%. The turnout in 2004 (year of RIES use) decreased to 17% of registered voters, with a 33% share of online ballots. This amounts to 70,000 online votes for Rinjland alone. In 2006, some 20,000 Dutch abroad registered to vote online. A total of 19,815 votes were cast online.
Voter Identification Mechanisms	Voters identify themselves on the system by typing their voting card number plus the last two digits of their year of birth. This combination is their private key.
Vote Verification Mechanisms	End-to-end verification.
Secrecy Protection	None.

Mechanisms	
Internet Voting System Provider	In 2004, for the two water board elections, the company TTPI. All RIES applications were designed and implemented by a company called Magic Choice, which owns the RIES source code. The RIES server and network infrastructure were hosted and managed by SURFnet.
Intellectual Property Rights of the Internet System	RIES is patented to Piet Maclaine Pont, a university professor under whose auspices it was developed, and the Rijnland water board.
Open/Closed Source Code	The source code has been published in June 2008; that is after the elections in which RIES was used. It was foreseen to make it available under a creative common license in 2008, but the end of electronic voting in the Netherlands made it irrelevant and it was not done.
System Testing and Certification Mechanisms	There was neither formal testing nor certification of the system. A series of testing was done over the years, but neither in a coordinated nor in a legally mandated way. The Digital security group of the Radboud University Nijmegen has performed an independent vote counting in 2004 and 2006 (ex-post verification) and has created its own control channel for voters (counted as cast). This group also audited the servers used in 2004.
Voting and Results Audit Mechanisms	RIES may boast to have been the first Internet voting system providing end-to-end verifiability. It was also based on the "zero-knowledge" approach, which means that anybody can build his own IT tools to verify the accuracy of the results.
Transparency Mechanisms	Most of the RIES technology is publicly available. The source code was published in 2008. Procedures for operating the system were however weak and the intervention of an insider on the votes could not be excluded.
Court Cases Against the Use of Internet Voting	None
References	http://www.openries.nl/ Hubbers, E, Jacobs, B., Schoenmakers, B., Tilborg, H. and Weger, B. – Description and Analysis of the REIS Internet Voting System, at http://www.win.tue.nl/eipsi/images/RIES_descr_anal_v1.0_June_24.pdf Jacobs, B. and Pieters, W. – Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment", at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.159.9956&rep=rep1&type=pdf OSCE – Netherland Parliamentary Elections 22 November 2006: OSCE/ODIHR Election Assessment Mission Report, at http://www.osce.org/odihr/elections/netherlands/parliamentary_2006

Data Sheet – Internet Voting
Spain

Introduction	Given that Barcelona claims to be a leading city regarding citizen participation, the modernization of its main streets was an excellent opportunity to deploy a project that would be based on an official Internet consultation. The citizenry had to decide whether to maintain the current avenue or to build a tramway alongside it, with two possible layouts. The Internet voting project was planned as a one off consultation. The project faced some critical situations (e.g. political polarization, identity theft, information mismanagement) that did not enhance the overall trustworthiness of the electoral procedure. The final outcome was not seen successful for a number of reasons: (i) Authentication Measures - While willing to increase turnout, the authentication mechanism allowed impersonations via someone getting a password with some personal data (e.g., ID number, birth date). When a prominent Catalan political leader showed up at the polling station, he was told that he had already voted the previous day. Moreover, mass media and other stakeholders also proved that fraud was also possible with other voters. However, the use of personal cellular phones was thought to avoid massive thefts and to track back those insiders discovered by actual voters. (ii) Information Management - At least one high profile issue was solved in a dubious way. Although the Mayor could not vote, he declared to the media that he had already cast his ballot and even maintained this statement afterwards. Although the e-voting application was not properly running, a technician actually advised the Mayor to declare that he had voted. Once a Catalan newspaper discovered the situation, the Mayor recognized that, although he thought that the ballot was sent, he still had some doubts and thus had to confirm whether his ballot had actually been cast. When he was told that the ballot has not been received by the server, he was forced to vote again. (iii) Lack of Political and Social Consensus - The project was controversial and there was no consensus on the opportunity, both to use the tramway and to organize the consultation itself. The technical problems discovered during the implementation of the project polarized stakeholders even more.
Years of Use	2010 (Barcelona). There have been other local consultations in Spain, but only in small municipalities and with uncertain legal frameworks. *MadridParticipa* (2004) might be the exception taking into account that it involved a big city, but it was more of a political initiative than a formal legal consultation.
Type of Elections/Referenda	Local citizen consultation (city of Barcelona)
Type and Status of the Internet Voting Option	Voting from PC's in unsupervised environments or voting from supervised kiosks. The use of Internet voting was only intended as a one-time use for the purpose of the citizen's consultation, but subsequent usage of Internet voting would have to face stakeholders' skepticism and distrust generated by the issues experienced.
Eligible Voters	Citizens over 16 years old legally registered in the general census of the population of Barcelona (including foreigners). No pre-registration was required.
Key features of the Internet voting system	Besides some patterns usually used in Internet voting consultations, this case included some specific features: (i) involvement of two e-voting providers (Indra and Scytl); (ii) only one voting channel (paper ballots were not used) and (iii) the

	appointing of an independent supervisory board (see below).
Other Voting Channels Available	Internet voting was the only channel available, either from home or from supervised environments.
Period of Internet Voting	Five days.
Legal Basis for Internet Voting	Besides the general legal framework (e.g., Barcelona Legal Act, Citizen Participation Regulations), there was a specific legal basis for this consultation (Local Decree / December 23rd 2009).
Internet Voting Usage	Total number of voters: 1,414,783 Total number of votes: 172,161 [12,17%] 48.3% from supervised environments
Voter Identification Mechanisms	Three authentication channels: (i) digital official certificates already accepted in other e-procedures with the Barcelona City Council (e.g., the one issued by CatCert, the official Catalan Authority for Digital Certificates), (ii) one-time password sent to a cellular phone (the citizens receive this password upon on-line request and providing their ID number, birth date and phone number) and (iii) partners' websites (e.g., Universities, banks) with their own authentication logins (the e-voting system is somehow embedded in the partner's websites and therefore citizens don't need new logins and passwords)
Vote Verification Mechanisms	None. Neither return codes nor E2E verification.
Secrecy Protection Mechanisms	Multiple voting was not used. There only was one revocation of a vote due to an impersonation. This option was technically available, but it was not published.
Internet Voting System Provider	Indra / Scytl Secure Electronic Voting
Intellectual Property Rights of the Internet System	Both providers fully retained the intellectual property of the Internet system. It was sold to the City Council on a one-time purpose basis.
Open/Closed Source Code	The source code could be disclosed after signing a Non-Disclosure Agreement (NDA). This was the case for the audit report issued by the Polytechnic University of Catalonia.
System Testing and Certification Mechanisms	An audit report issued by the Polytechnic University of Catalonia (UPC).
Voting and Results Audit Mechanisms	Neither return codes nor E2E were used.
Transparency Mechanisms	A supervisory board (*Mesa de Seguiment i Garanties*) was appointed by the City Council with external and independent members. The Board legally monitored the whole process.
Court Cases Against the Use of Internet Voting	Only one due to an impersonation. The lawsuit is still ongoing at the time of writing.

References	http://www.bcn.cat/diagonal/index.html

Data Sheet – Internet Voting
Switzerland-Geneva

Introduction	The Internet voting project is managed at the federal level for federal ballots, while cantons are autonomous when it comes to cantonal or municipal ballots. The long-term objective (2020 or so) of the Confederation is to enable all Swiss citizens to be able to vote online, next to postal voting and voting in polling stations. But security comes first and there is not an officially binding timetable for the extension of Internet voting to the whole country. In 2000, the Confederation invited interested cantons to develop a system with federal support. Three cantons came forward: Geneva, Neuchâtel and Zurich. Only Geneva developed its own system and owns it. Zurich owns its system, but it was developed and is run by Unysis. Neuchâtel relies on Scytl. This diversity is a consequence of the federal nature of the country. The Confederation considered that given the existence of 26 cantonal laws and procedures relating to political rights, one single system would not have been flexible enough to be implemented in so many different contexts. We will consider here the Geneva system, the most developed among the three and the most transparent.
Years of Use	2003, 2004, 2005, 2006, 2008, 2009, 2010, 2011, in all these cases for referenda, except three administrative elections. As of August 2011, 19 referenda had been organized using Internet voting.
Type of Elections/ Referenda	2003: municipal referenda. 2004: municipal and federal referenda. 2005: cantonal referendum. 2006: election of the council of the Geneva Technical School. 2008: cantonal and federal referenda. 2009: cantonal and federal referenda. 2010: cantonal and federal referenda. 2011: cantonal and federal referenda and election of the council of the Geneva University and of the delegates of the Geneva libraries staff.
Type and status of the Internet Voting Option	Voting by PCs from unsupervised environments. There is no kiosk voting and no way to vote in supervised environments. Internet voting is offered for all referenda.
Key features of the Internet voting system	The Geneva Internet voting system relies on a simple architecture, the extensive use of a quantum generator to produce the various cryptographic keys and voters' identifying features values used during the voting session, as well as on a strict division of duties and responsibilities between the various services of the administration and the Central Electoral Commission. It uses symmetric and asymmetric keys and encrypted ballots. A mixing process is applied to the ballots before their counting. The SSL protocol has been shown to be susceptible to "man in the middle" attacks. That is why the Geneva system implements a combination of several security techniques called "secure channel": mutual SSL protocol, surencryption of the data and authentication of messages. As current web browsers do not offer the functions required to implement these features, the Geneva system uses a java applet that is downloaded to the voter's computer.

	An integrity meter recognized only by the voting system ensures that no vote is added or subtracted without this being seen. The electronic ballot box is sealed with a key owned by the Central Electoral Commission.
Eligible Voters	All Geneva-registered voters living abroad can vote online provided they live in the European Union or in one of the countries that has ratified the Wassenaar agreement on the trade of dual-use (civilian and military) goods and services (www.wassenaar.org), as cryptography can be considered as a military item. For federal referenda, the Confederation imposes a cap to Geneva residents entitled to vote online. No more than 20% of registered resident voters may be offered online voting. The selection is done by choosing 10 to 12 municipalities whose registered voters together represent 20% of the Geneva voters. Referenda of all levels (federal, cantonal and municipal) are organized simultaneously; the highest-level legal regulation applies. Therefore, only when there is no federal referendum can online voting be offered to all Geneva citizens. That has been the case only twice to-date: In May 2011 and again in November 2011. For cantonal and municipal referenda, no restrictions apply. For municipal referenda, foreign residents may also vote, as they were granted political rights at the municipal level in 2004. No pre-registration is needed.
Other Voting Channels Available	Advance postal voting (three weeks before ballot days for federal ballots, two weeks for cantonal and municipal ones) and polling station on election day.
Period of Internet Voting	The 28 days preceding the opening of the polling stations. Online voting closes midday on the Saturday prior to the polling stations opening day.
Legal Basis for Internet Voting	In the federal law: article 8a of the Federal Act on Political Rights (http://www.admin.ch/ch/e/rs/c161_1.html) and article 27a to 27q of the Federal Regulation on Political Rights. In the Geneva cantonal law: article 48 of the Geneva Constitution and article 56, 57, 60, 64, 65a, 67 and 74 of the Geneva Act on Political Rights. To be noted: the constitutional disposition on Internet voting has been adopted in a popular vote in February 2009 with 70.2% of all cast votes in favor. This disposition also foresees the creation of a Central Electoral Commission (CEC), as the members of the cantonal parliament who wrote it felt Internet voting required independent supervision.
Internet Voting Usage	Internet voting regularly represents some 20% of the votes cast in any given referenda. 18 January 2003: 1,162 eligible voters, turnout 63.7%, share of online votes 44%. 29 November 2003: 2,521 eligible voters, turnout 59%, share of online votes 29%. 17 April 2004: 9,049 eligible voters, turnout 44%, share of online vote 26%. 12 June 2004: 9,180 eligible voters, turnout 29%, share of online votes 22%. 25 September 2004: 22,000 eligible voters, turnout 57.1%, share of online votes 21.8%. 23 October 2004: 1,382 eligible voters, turnout 59.5%, share of online votes 32%. 27 November 2004: 41,200 eligible voters, turnout 43.9%, share of online votes

	22.4%. 23 April 2005: 88,000 eligible voters, turnout 44.1%, share of online votes 20.3%. 23 November 2006: 945 eligible voters, turnout 29%, share of online votes 100% (no other option was offered). 20 November 2008: 43,690 eligible voters, turnout 44.5%, share of online votes 14%. 17 May 2009: 46,500 eligible voters, turnout 43%, share of online votes 16.9%. 27 September 2009: 59,650 eligible voters, turnout 48.6%, share of online votes 19.6%. 29 November 2009: 59,360 eligible voters, turnout 56.4%, share of online votes 17.7%. 7 March 2010: 63,530 eligible voters, turnout 48.9%, share of online votes 19.2%. 26 September 2010: 64,000 eligible voters, turnout 41%, share of online votes 19.3%. 28 November 2010: 64,200 eligible voters, turnout 54.9%, share of online votes 20.5%. 13 February 2011: 64,830 eligible voters, turnout 48.4%, share of online votes 21.8%. 25 March 2011: eligible voters 164, no other data (election of the representatives of the Geneva libraries staff). 15 May 2011: 241,780 eligible voters, turnout 40%, share of online votes 22.1%. 18 May 2011: 21,000 eligible voters, turnout 14.5%, share of online votes 100% (no other option was offered for the election of the Council of the Geneva University). (Source: www.ge.ch/evoting/doc/list_of_GVA_ballots.pdf).
Voter Identification Mechanisms	For each voting operation, the voter receives by post a single-use voting card containing a unique voting card number enabling them to be identified in the voting management system, irrespective of the voting channel (electronic, postal or polling station) they choose. So that this crucial information is not compromised online, it is never exchanged. Instead, an imprint of the voting card number is sent out. This imprint is obtained by applying a cryptographic hash function to the voting card number. For the online vote, the voter number and a password are completed by the insertion by the voters in the system of two shared secrets, not present on the voting card: their birth date and their municipality of origin.
Vote Verification Mechanisms	None for the voter. There is, however, in the system a special constituency where the CEC casts Internet votes and records their content on a paper form. Before counting the electronic votes, after the ballot closure, the results of this constituency are first checked against their paper record to ensure that the system does not bias the outcome.
Secrecy Protection	The voter register uploaded into the system is fully anonymous. Voters are only identified by their one-time voter number.

Mechanisms	
Internet Voting System Provider	The system was developed in 2002 by Hewlett Packard, after a call for tender (actually, only one engineer at HP worked on the project). HP stopped being involved in the system in 2004, after this engineer went into retirement. Since then, the system has been developed by the State of Geneva IT department, with the support of a very few external companies, the main one being the Geneva Solution.
Intellectual Property Rights of the Internet System	The State of Geneva owns the intellectual property rights.
Open/Closed Source Code	According to article 60 of the Geneva Act on Political Rights, the source code publication is not regulated by the Public Information Act (which rules that all State documents are public, bar explicitly stated exceptions). The Geneva Act on Political Rights states, however, that the source code can be tested by any Geneva citizen who justifies a scientific and ideal interest and commits himself to confidentiality. The conditions for accessing the source code are set by the government. Nobody has requested this access so far and the government has not promulgated conditions. The CEC and any expert it mandates can freely access the source code.
System Testing and Certification Mechanisms	The special constituency dedicated to the CEC has been mentioned above. Next to it, before each ballot, the system is tested using predictive data. The principle is the same as for the CEC's constituency. A mock election or referendum is conducted on the system with preset votes, so that the operators know what results to expect from the system during the counting process. In addition, voluntary mistakes are made in the voting procedure to see if and how the system reacts to them. All these tests are recorded in a large binder that is open to the CEC. Only after the successful completion of these tests is the system sealed for the upcoming ballot. Article 60 of the Geneva Act on Political Rights also foresees a triennial audit, whose results are public. This article was adopted in 2010 and the first audit is due in 2012. Finally, the administration regularly mandates private companies to perform tests and audits of the system. Only the CEC can see their reports.
Voting and Results Audit Mechanisms	Forensic statistic tests are systematically performed on the result of the electronic voting channel.
Transparency Mechanisms	The special constituency dedicated to the CEC.
Court Cases Against the Use of Internet Voting	There were two legal procedures against Internet voting. After the May 2009 referendum, when the introduction of biometric passports was accepted nationwide by a margin of 5,680 votes out of 1.9 million votes cast, several citizens in different cantons appealed to their cantonal government first and then to the federal court (the supreme court in Switzerland). They opposed biometric passports and argued that such a close result should be considered an irregularity and that either a recount or a new ballot should be organized. The use of Internet voting was, in their eyes, an aggravating factor (only three out of the 26 cantons had provided Internet voting to their citizens, under the restrictions evoked under the chapter "Eligible voters"). The federal court dismissed the lawsuits both for lack of evidence of irregularity and lack of legal basis to mandate a recount

	or a new election. In May 2011, in Geneva, when for the first time all Geneva citizens could vote online, a citizen went to court after the vote to have the election annulled. He said that because of the inherent flaws of Internet voting, the outcome of the ballot could be the result of massive fraud. He didn't bring any evidence in support of this theory. The court dismissed his case on formal grounds (he didn't introduce his case soon enough after having known that all Genevans could vote online in May 2011).
Reference	Brochure "The Geneva Internet voting system", www.ge.ch/evoting/english/doc/passport_evoting2010.pdf "Uncovering the veil on Geneva's Internet voting solution", www.ge.ch/evoting/english/doc/Flash_IT_vote_electronique_SIDP_final_english.pdf "Analysis of the 26th September 2004 ballot as held in four Geneva municipalities", www.ge.ch/evoting/english/doc/rapports/rapport_26sept_english_final.pdf

Data Sheet – Internet Voting
United Kingdom

Introduction	Long standing concern about the need to update a number of electoral procedures led to a report (Electoral Law and Administration) from the Home Affairs Select Committee, in 1997-8 which addressed many of the issues of concern. A Home Office working party produced a final report in October 1999 which recommended change in a number of areas, including the introduction of the possibility of election pilots for local government elections. The Representation of the People Act 2000 implemented the recommendations and included measures that enabled local authorities to apply for permission to pilot a range of new electoral arrangements for local elections which would assess whether different polling procedures would improve turnout at these elections. Under the provisions of the Act, pilot schemes cannot be used when there is more than one type of election held on the same day. As a result, there were no pilots when the local elections were combined with the General Elections in 2001 and 2005. Among the various pilot schemes that were piloted, several addressed the issue of how to vote. These included: • automated voting or vote counting, replacing manual voting and vote counting with electronic polling machines or ballot paper scanners • telephone voting, using domestic telephones linked to automatic voice recognition and recording equipment at one or more central locations • electronic voting, on-line from publicly sited terminals and other access points such as digital television using the Internet Pilot scheme proposals had to consider how to safeguard the integrity of a remote voting arrangement and the resilience and effectiveness of technology supporting such solutions. Voter reaction to electronic delivery of services was also a factor to be considered in preparing proposals. A particular consideration in evaluating the scope for rolling out more technologically based schemes was likely to be the extent to which the proposals depended upon assumptions about the technical infrastructure of local government.
Years of Use	2002 to 2007 except for 2005 (see 2nd paragraph above)
Type of Elections/ Referenda	Local government elections held largely in England.
Type and Status of the Internet Voting Option	Internet voting was available by any access channel to the Internet including kiosk voting and voting in supervised environments. After the 2007 pilots no further experiments into alternative voting channels have been conducted during UK elections.
Key features of the Internet voting system	The various types of system used in the pilots generally followed the practice of codes being issued to electors by mail. These codes then had to be entered at sign in to allow access to the Internet voting system and the ability to cast a vote.
Eligible Voters	All registered voters. In most pilots, the use of Internet voting was optional and other remote methods such as telephone or SMS were offered. Conventional voting in polling stations was available for those who did not wish to use alternative methods for voting.

<table>
<tr><td><b>Other Voting Channels Available</b></td><td>See above. In addition, postal voting is available on demand in the UK.</td></tr>
<tr><td><b>Period of Internet Voting</b></td><td>Varied from scheme to scheme, but in most cases was available from about two weeks before election day and up to and including that day.</td></tr>
<tr><td><b>Legal Basis for Internet Voting</b></td><td>Provisions in the Representation of the People Act 2000 enabled local authorities to apply for permission to pilot a range of new electoral arrangements. Where applications were approved by the Secretary of State, separate statutory orders were created for each pilot scheme.</td></tr>
<tr><td><b>Internet Voting Usage</b></td><td>In 2003, the following usage was reported for the 14 remote e-voting pilots:
<table>
<tr><th>Channel</th><th>Overall usage</th><th>Usage where channel available</th></tr>
<tr><td>Polling station (paper)</td><td>34.6%</td><td>67.6%</td></tr>
<tr><td>Postal voting</td><td>40.4%</td><td>40.4%</td></tr>
<tr><td>Internet</td><td>12.6%</td><td>12.6%</td></tr>
<tr><td>Telephone</td><td>6.5%</td><td>7.1%</td></tr>
<tr><td>Text message</td><td>1.4%</td><td>3.8%</td></tr>
<tr><td>Digital TV</td><td>0.2%</td><td>1.2%</td></tr>
<tr><td>Kiosk (where only in-person method)</td><td>3.7%</td><td>77.3%</td></tr>
<tr><td>Kiosk (where one channel in multi-channel pilot)</td><td>0.7%</td><td>1.3%</td></tr>
<tr><td>All remote e-channels</td><td>20.7%</td><td>N/A</td></tr>
</table>
Statistics for other years show broadly similar results.</td></tr>
<tr><td><b>Voter Identification Mechanisms</b></td><td>Voters identified themselves on the system by typing the pin numbers sent to them via mail.</td></tr>
<tr><td><b>Vote Verification Mechanisms</b></td><td>Some systems provided a code to confirm that the vote has been received.</td></tr>
<tr><td><b>Secrecy Protection Mechanisms</b></td><td>None.</td></tr>
<tr><td><b>Internet Voting System Provider</b></td><td>• Accenture
• BT
• DRS (Data and Research Services)
• ES&S (Election Systems and Software)
• Indra
• OPT2VOTE
• Software AG
• Strand Enterprises</td></tr>
</table>

	• Tata • Unisys
Intellectual Property Rights of the Internet System	In general terms, the systems are owned by the various suppliers.
Open/Closed Source Code	Generally closed, particularly as these were all pilot schemes.
System Testing and Certification Mechanisms	There was neither formal testing nor certification of the systems.
Voting and Results Audit Mechanisms	Return codes were not generally used. There were no formal mechanisms.
Transparency Mechanisms	Observers were permitted from 2006. Reports from the Open Rights Group on their observation experiences can be found at: http://www.openrightsgroup.org/ourwork/successes/evoting
Court Cases Against the Use of Internet Voting	None
References	Further information about the UK pilots can be found at: 1. House of Commons Library paper – http://www.parliament.uk/documents/commons/lib/research/briefings/snpc-04397.pdf 2. Electoral Commission report on 2003 Pilots – http://www.aea-elections.co.uk/downloads/ec_report_on_2003_pilots.pdf 3. Public Opinion report by Mori on 2003 Pilots – http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0017/16109/MORIPublicopinionandthe2003electoralpilotschemes_10314-8349__E__N__S__W__.pdf 4. E-Democracy Blog "Internet Voting – History of a failed policy" – http://www.edemocracyblog.com/edemocracy-blog/internet-voting-history-of-a-failed-policy/

Data Sheet – Internet Voting
United States-West Virginia

Introduction	The West Virginia Internet pilots were designed to comply with the electronic transmission elements of the Military and Overseas Voter Empowerment (MOVE) Act. The United State Congress passed the MOVE ACT as part of the National Defense Authorization Act, in 2009. The MOVE Act was designed to strengthen the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), signed in 1986. UOCAVA protects the right of military service members to vote in federal elections regardless of where they are stationed. Specifically, the MOVE Act required that states transmit any requested absentee ballots to UOCAVA-covered voters no later than 45 days before a federal election. The first pilot was for West Virginia's 2010 primary election. These pilots were initially limited to five West Virginia counties, all of whom were required to submit a letter of request to participate to the Secretary of State's office. After the primary, three more counties submitted requests, and all eight participated in the program for the 2010 general election. Although the pilot experienced no problems, it attracted some criticism from security experts who voice concern over Internet voting in general. This was heighted by a high-profile test by the Washington, DC Board of Ethics and Elections (DCBOEE). DCBOEE ran a mock election in which they encouraged hackers to thwart the system to test its vulnerability. After a team of students from the University of Michigan successfully hacked the system, DCBOEE abandoned the project. West Virginia's Secretary of State, Natalie Tennant, has stated she wished to convene a study committee, which can address concerns and recommend future actions.
Years of Use	2010
Type of Elections/Referenda	Primary and General Election. This includes presidential, federal, state and county ballots.
Type and Status of the Internet Voting Option	Unsupervised, remote Internet voting. The West Virginia Secretary of State has requested that a study committee evaluate potential security issues before moving forward with the system in future elections.
Brief Description of Internet Voting System	Eligible voters first submitted a Federal Post Card Application (FPCA) or the West Virginia Electronic Voting Absentee Ballot Application. After this, the voters received an email from either the county clerk (of the county they were a citizens of), or the voting system vendor. This email contained a username and URL to a secure website. The voter could then cast a ballot with this information and, upon completion, receive a receipt code that verifies the vote was processed correctly. After the ballot was cast, it was stored in an encrypted format on a host server. It stayed there until election night, when it was transferred to a stand-alone, non-networked computer to be decrypted. The decryption process disassociates voted ballots from any voter-identifying information and is done by a few "key holders" who are usually County Commissioners. The key holders enter unique passwords into the computer. Only a combination of multiple passwords will unlock the data. Decrypted ballots are then printed and included in the central count of all absentee ballots. Internet vote totals are not released by themselves. This is done so the low number of Internet voters does not threaten the secrecy of the ballot. In Mason County, for example, only one voter cast an online ballot during the general election.
Eligible Voters	Military and overseas voters who are citizens of pilot counties in the state of West

<table>
<tr><td></td><td>Virginia and covered by the federal Uniformed and Overseas Citizens Absentee Voting Act. Voters had to submit a Federal Post Card Application (FPCA) or West Virginia Electronic Voting Absentee Ballot Application.
The counties of Jackson, Kanawha, Marshall, Monongalia and Wood participated in both the primary election on May 11, 2010 and the general election of November 2, 2011. The counties of Mason, Monroe and Putnam participated during the general election.</td></tr>
<tr><td><b>Other Voting Channels Available</b></td><td>Registered overseas voters could also be sent a mail ballot for postal voting. In addition, all 55 counties in West Virginia piloted an online ballot delivery program where the voter could print a ballot from online, and then return by standard mail, fax or e-mail.</td></tr>
<tr><td><b>Period of Internet Voting</b></td><td>For the primary election, the period was Tuesday, March 30, 2010 to Tuesday, May 11, 2010 at 7:30 p.m.</td></tr>
<tr><td><b>Legal Basis for Internet Voting</b></td><td><i>Article 3B - Uniformed Services and Overseas Voter Pilot Program of the West Virginia Code (§3-3B-3 W.Va. Code) mandated the Secretary of State implement and evaluate an Internet voting pilot program for military and overseas voters to comply with the 2009 Military and Overseas Voters Empowerment (MOVE) Act.</i>
<i>The MOVE Act strengthened the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), which UOCAVA protects the right of service members to vote in federal elections regardless of where they are stationed. The MOVE Act mandates that states transmit any requested absentee ballots to UOCAVA-covered voters no later than 45 days before a federal election, assuming the request has been received by that date.</i></td></tr>
<tr><td><b>Internet Voting Usage</b></td><td>For the general election, there were 165 voter applicants with 125 of those casting ballots.
<table>
<tr><th><u>County</u></th><th><u>Votes Cast</u></th><th><u>Vendor</u></th></tr>
<tr><td><b>Jackson</b></td><td>10</td><td>Scytl</td></tr>
<tr><td><b>Kanawha</b></td><td>35</td><td>Everyone Counts</td></tr>
<tr><td><b>Marshall</b></td><td>9</td><td>Scytl</td></tr>
<tr><td><b>Mason</b></td><td>1</td><td>Scytl</td></tr>
<tr><td><b>Monongalia</b></td><td>22</td><td>Everyone Counts</td></tr>
<tr><td><b>Monroe</b></td><td>3</td><td>Everyone Counts</td></tr>
<tr><td><b>Putnam</b></td><td>15</td><td>Everyone Counts</td></tr>
<tr><td><b>Wood</b></td><td>30</td><td>Everyone Counts</td></tr>
</table></td></tr>
<tr><td><b>Voter Identification Mechanisms</b></td><td>Voters apply to vote online through their county clerk, who is responsible for determining eligibility of the voter. This application is done through the Federal Post Card Application (FPCA) or the West Virginia Electronic Voting Absentee Ballot Application Voters. The county then supplies the voter with a password and URL for the secure website, where the elector can cast a ballot. The voter enters the provided identifier, along with additional personally-identifying information, into the website in order to access the correct ballot.</td></tr>
<tr><td><b>Vote Verification Mechanisms</b></td><td>Voters receive a receipt code. The code does not allow a voter to view how they cast their ballot, only that the vote was received and processed. The system would let the voter know if their ballot was rejected.</td></tr>
</table>

Secrecy Protection Mechanisms	The online voting systems ran on redundant servers, located both locally and remotely. This allowed the system to continue to operate if one went down. Each system used 2048-bit encryption, and a Secure Socket Layer access to the application. The number of election officials who received data provided by Scytl and Everyone Counts was kept to a minimum and each are bound by confidentiality statements. The systems used separate encryption/decryption algorithms for creating keys to link the voter and ballot data.
Internet Voting System Provider	Everyone Counts and Scytl
Intellectual Property Rights of the Internet System	Everyone Counts and Scytl
Open/Closed Source Code	Closed source
System Testing and Certification Mechanisms	The West Virginia Secretary of State's office was responsible for procuring the equipment. A report from the Secretary of State notes that the two systems, both Everyone Counts and Scytl, did not submit their processes for validation by the National Institute of Standards and Technology's (NIST) Cryptographic Algorithm Validation Program (CAVP); however, there is no current requirement to do so.
Voting and Results Audit Mechanisms	Aside from the receipt code provided once a ballot is cast, no other mechanisms appear to have been implemented.
Transparency Mechanisms	None
Court Cases Against the Use of Internet Voting	No lawsuits were found.
Key Reports/Documents	West Virginia Secretary of State, legislative report *West Virginia Uniformed Services and Overseas Citizen: Online Voting Pilot Project* (Charleston, West Virginia: January 19, 2011)

Annex 2 – Data Sheet: Supervised Internet Voting:

- Finland

Data Sheet – Internet Voting
Finland

Introduction	In 2008 Finland started an Internet voting project that encompassed three municipalities during their local elections. Citizens should still show up at the polling station to cast a ballot that would be afterwards electronically sent to a common server for these three municipalities. The main goal was to speed up the process and to enhance the security of ballot boxes used during the advanced period. A usability issue led to 200 votes not being properly registered, with voters mistakenly leaving the voting kiosks before completing the voting process. This led to the withdrawal of the results in these three municipalities and the conduct of a fresh election only using paper ballots. The University of Turku issued an audit report, but other stakeholders refused to sign the Non Disclosure Agreement (NDA) proposed by the suppliers. The total costs of the project from 2005-2008 were 1,630,550 Euro. This consisted of costs for; the IT supplier – 1,330,872 Euro; Auditing costs – 141,882 Euro; Materials - ballot booths (70,102 euro) and voting cards (10,076 euro); and compensations for extra costs to the pilot municipalities - 77,618 euro.
Years of Use	2008
Type of Elections/Referenda	Local (only three municipalities: Karkkila, Kauniainen and Vihti)
Type and Status of the Internet Voting Option	Supervised voting in a polling stations environment. Now discontinued. Some voters left the polling station without completing the casting of their vote, although they believed that the voting session had already ended. As a consequence, the final number of votes did not match with the number of voters marked on the electoral roll and the Court decided to repeat the election. Due to this poor experience, no further trials or implementation has proceeded in Finland.
Key features of the internet voting system	Besides some patterns usually used in i-voting systems, this case included some other specific features: (i) supervised environments and (ii) interesting legal issues. Although ballots were remotely transmitted to a central server, citizens had to cast them within supervised environments, due to prudent concerns given that it was the first time using i-voting. After the re-run, the Finnish government decided to rather concentrate new e-voting projects in remote and non-supervised channels. Secondly, the lawsuits resulted in a re-run election being held in the three municipalities and also generated interesting legal reasoning on the consequences of e-voting usability.
Eligible Voters	Only voters from the three selected municipalities (ca. 34000), no pre-registration was required.
Other Voting Channels Available	Paper based ballots
Period of Internet Voting	Advanced election period (from 15th to 21st October) and also during the election day (October 26).
Legal Basis for Internet Voting	"To enable the pilot project the Act amending the Election Act (880/2006) was enacted. The Act is in force from 1 January 2007 to 31 December 2008" (www.vaalit.fi/sahkoinenaanestaminen/en/yleistietoa.html) Amendment 880/2006: www.finlex.fi/fi/laki/alkup/2006/20060880 (only in Finnish). It

<table>
<tr><td></td><td>had a temporary validity, only for this pilot.</td></tr>
<tr><td><b>Internet Voting Usage</b></td><td>
<table>
<tr><th></th><th>Voters</th><th>Votes</th><th>I-Votes</th><th>Paper ballots</th></tr>
<tr><td>Karkkila</td><td>7,112</td><td>4,117</td><td>2,165</td><td>1,952</td></tr>
<tr><td>Kauniainen</td><td>6,391</td><td>4,623</td><td>2,982</td><td>1,641</td></tr>
<tr><td>Vihti</td><td>20,559</td><td>11,617</td><td>7,087</td><td>4,530</td></tr>
<tr><td><b>Total</b></td><td><b>34,062</b></td><td><b>20,357</b></td><td><b>12,234</b></td><td><b>8,123</b></td></tr>
<tr><td colspan="5">NB - 4,985 of the i-votes were cast during the advanced period of voting.</td></tr>
</table>
Source: Finnish Government</td></tr>
<tr><td><b>Voter Identification Mechanisms</b></td><td>After the exhibition of a valid ID, the voter receives an electronic card with which s/he will operate with the voting machine.</td></tr>
<tr><td><b>Vote Verification Mechanisms</b></td><td>None. Although the Finnish Government asserted that, “The electronic voting system has been constructed under the supervision of the Ministry of Justice. This way the voter can be confident that the system works appropriately and gives the correct election result” (www.vaalit.fi/sahkoinenaanestaminen/en/ukk/ukk8.html), no formal mechanisms for vote verification were provided.</td></tr>
<tr><td><b>Secrecy Protection Mechanisms</b></td><td>The same protections as for paper balloting since the Internet voting took place in supervised environments. The link between voters' ID and the vote's value is handled by the software and it is broken by the mixing process conducted at the beginning of the tally under the supervision of private keyholders.</td></tr>
<tr><td><b>Internet Voting System Provider</b></td><td>TietoEnator / Scytl Secure Electonic Voting. The voting platform was also linked to the Election Information System normally used by the Election Authorities in Finnish elections.</td></tr>
<tr><td><b>Intellectual Property Rights of the Internet System</b></td><td>Both providers fully retained the intellectual property of the Internet System. It was provided to the government on a one-time only basis.</td></tr>
<tr><td><b>Open/Closed Source Code</b></td><td>“the source code is not open, and only the most critical sections were reviewed” [<i>Audit report on pilot electronic voting in municipal elections</i>, University of Turku, p. 3] after signing a Non Disclosure Agreement (NDA) that other stakeholders (e.g. EFFI) refused due to its limited and unfair content.
Turku's report available at:
www.vaalit.fi/uploads/5bq7gb9t01z.pdf [last accessed August 18, 2011]
The NDA which was rejected by some stakeholders can be found at:
winston.effi.org/system/files?file=22413-NDA-muut.pdf   [last accessed August 18, 2011]</td></tr>
<tr><td><b>System Testing and Certification Mechanisms</b></td><td>Beyond the usual tests carried out in any technical implementation, neither specific test measures nor a formal certification were conducted.</td></tr>
</table>

Voting and Results Audit Mechanisms	There was an external audit conducted by the University of Turku. The ballot box is protected by a private cryptographic key that is shared by several keyholders. The ballot box can only be opened joining again these keyholders.
Transparency Mechanisms	Some features of the e-voting system were available after signing a NDA. Moreover, the Ministry of Justice received some requests for access to the e-voting documents, but it refused them partly because the requested documents contained descriptions of the security solutions of the e-voting system and proprietary information. According to the Act on the Openness of Government Activities (621/1999), it was not possible to publish such documents which contained business secrets or trade secrets of the suppliers or documents relating to or affecting the realization of the security arrangements and data communications systems, unless it was obvious that access would not compromise the achievement of the objective of the security arrangements. When opening the electronic ballot box, the screens were reflected on two silver screens so that everyone present could see what commands were given and how the computers were functioning. Source: Finnish Government
Court Cases Against the Use of Internet Voting	1) Supreme administrative court, case number 1683/1/08. 2) Five appeals dismissed by the Helsinki Administrative Court / 29 January 2009 3) Four appeals accepted by the Supreme Administrative Court / KHO:2009:39 (687/1/09), 9 April 2009 / www.kho.fi/paatokset/46372.htm Decision 1 refers to a risk analysis whose disclosure had been refused by the Ministry. Decisions 2 and 3 analyze votes lost by usability issues. The first one backed the results, but the second withdrew them. The elections have since been repeated using only paper ballots.
References	Finnish Ministry of Justice Website on Electronic Voting Pilots - www.vaalit.fi/42735.htm *and* www.vaalit.fi/sahkoinenaanestaminen/en/yleistietoa.html.

Annex 3 – Internet Voting Case Studies

Estonia

After a short period of independence in the early 1920s Estonia regained its independence in 1991, simultaneously with Lithuania and Latvia. Right now Estonia is member of the European Union and its political system is based on a parliamentary system of governance.

The first governments quickly adopted an e-strategy pursuing the intensive use of New Technology for Information and Communication (NTICs) within public administration. A decade later, Estonia remains at the forefront of e-government. Therefore, the introduction of Internet voting was considered as a natural objective in this overall e-strategy, which is now seen as a cornerstone of public affairs.

Previously the Estonian Government also decided to distribute an e-ID card that includes cryptographic protocols to allow remote authentication and digital signatures. The successful deployment of this token has been essential for the Internet voting project because it mitigates the challenge of remotely authenticating the voter.

Estonia became the first country to offer Internet voting to the entire electorate for nationwide, binding elections. This has now happened in local (2005, 2009), parliamentary (2007, 2011) and European (2009) elections. The first three elections were carried out without major criticisms and with a growing percentage of Internet voters. The 2011 parliamentary elections saw a significant increase in the usage of Internet voting (with over 24 percent of all votes cast using the Internet) and a parliamentary committee has been established to evaluate the system and suggest potential improvements.

The OSCE's Office for Democratic Institutions and Human Rights (ODIHR) 2011 *Parliamentary Election Observation Report* made a number of recommendations about the improvement of the Internet voting system in Estonia. These suggestions included the formalization of the overall procedure to include more detailed legal regulations, formal reports for software deployment and testing measures or data protection guarantees. In addition, the assessment mission also underlined the necessity to enhance in-house IT expertise so the electoral authorities could monitor the overall system and delegate "the responsibility for certification of the Internet voting system to an independent public body that would evaluate and then digitally sign the final version of the Internet voting software and publish a public evaluation report" (OSCE/ODIHR 2011: 14). While the Estonian project has a successful history so far, it needs to continue to be developed in order to meet future challenges, as well as emerging international electoral standards with respect to Internet voting. Better legislation, a transparent policy and formalized procedures, aspects identified by the assessment mission, clearly demonstrate that the Estonian authorities need to be aware of potential, even necessary, improvements to the system in the future.

Surveys conducted since 2005 by the European University Institute of Florence about Internet voting in Estonia also include some recommendations that could be taken into account by Estonian electoral authorities (Trechsel 2011: 21). In 2009, for instance, the survey report argued for a certification procedure for the Internet voting system and also pointed out that electronic voting should not be used only in future elections. It should also be considered for broader democratic goals, such as enhancing civic e-participation (Trechsel and Vassil 2010).

As outlined above, no restriction is foreseen regarding eligible voters and no pre-registration is required. However, voters need to have a valid ID (ID card, digital ID or mobile ID). Internet voting turnout has increased from 1.9 percent of all votes cast at its introduction in the 2005 local elections to 24.3 percent of all votes cast in the 2011 parliamentary elections (see Figure 11 below for additional information on Voting Turnout).

Figure 11 - Internet Voting Statistics for 2005, 2007, 2009 and 2011 Elections

	2005 LE	2007 PE	2009 EPE	2009 LE	2011 PE
I-votes counted	9,287	30,243	58,614	104,313	140,846
Number of all votes counted	496,336	550,213	396,982	658,213	580,264
I-votes among all votes	1.9 %	5.5 %	14.7 %	15.8 %	24.3 %
I-votes among total advance votes given	7.2 %	17.6 %	45.4 %	44 %	56.4 %
I-votes cast abroad [51 countries in 2007, 66 in EPE and 88 (only temporary abroad) in LE 2009, 105 in 2011]	NA	2 %	3 %	3 %	3.9 %

Source: www.vvk.ee/voting-methods-in-estonia/engindex/statistics, (OSCE/ODIHR 2011: 8).

Internet voting is only available before Election Day, during an advanced voting period, normally one week. Voters may cast several ballots during this period and only the last one will be considered as valid for the official tally. Various paper ballot options are also available. Voters can cast an advanced paper ballot. Estonians living abroad may cast their ballot by post or vote at an embassy abroad. Voting from ships is also offered.

Those voting by Internet will have their names removed from the electoral register in their polling station, but any paper ballot cast in the advanced period will be counted, canceling any Internet ballot cast by the voter. The strategy of allowing multiple votes and the primacy of the paper ballot is intended to protect the freedom of the voter by dissuading vote coercers on the basis that they will never know which ballot will be included in the tally.

Internet voters identify themselves with a smart ID systems that can be the national ID card, a digital one without picture or even a mobile ID (a new authentication channel using mobile phones with specific SIM cards that was introduced in 2011). Once authenticated, the citizen casts the ballot through a platform that sends it to a central database. The vote is digitally signed (inner envelope) and inserted in another virtual and signed "envelope" (outer one) that contains the identification of the voter and the session log.

While there is one Electoral Law per election type, the respective electoral codes do not contain detailed or comprehensive regulations pertaining to Internet voting. In addition, a Decree issued by the National Electoral Committee (NEC) and internal operational guidelines offers more detailed guidelines about

Internet voting procedures. The Internet voting system was initially challenged based on a lack of uniformity between different voting channels due to Internet voters being able to cast multiple votes. The case was brought before the Estonian Supreme Court because of concerns that only Internet voters would have the chance to alter their vote and this inequality would be unacceptable from a democratic point of view. The Estonian Supreme Court stated that this measure is sufficient to mitigate possible undue influence over voters. The Court also argued that it complies with the principle of equality, understood in this case as a certain uniformity of opportunity between voting channels. Noting that uniformity is not an absolute principle for electoral matters, the Supreme Court concluded that in cases of voting from unsupervised environments, multiple voting is a reasonable way to address concerns linked to the principle of vote secrecy and therefore represented a reasonable limitation of the equality of voting rights (Estonian Supreme Court 2005: § 27).

Trust in Internet Voting

Electoral management in Estonia is led by the National Electoral Committee (NEC), but there are other stakeholders directly involved in the electoral process. *Cybernetica AS*, for instance, has been contracted as the main supplier of the Internet voting system. The Internet voting system is also tested either by the NEC or by other public agencies such as, in 2011, the *Cyber Defence League* (CDL). An independent programmer has also been contracted to test the software. However, the relevant reports are kept secret in some cases (OSCE/ODIHR 2011: 10). Finally, the Riigikogu IT Department also plays an important role since the NEC itself does not have computer experts able to handle the overall procedure including tenders, management and supervision.

Although Internet voting devices and procedures are not formally certified by independent firms, the NEC always hires an auditing company (e.g. KPMG Baltic in 2011) whose goal is to verify that each relevant stakeholder is following the rules and criteria previously defined in the operation manual. It is worth stressing that KPMG's task is limited to verifying compliance with these documents and it is not empowered to conduct an independent assessment of the suitability of these documents.

Finally, the NEC organizes information and training sessions for observers and for the general public, although a Non-Disclosure Agreement (NDA) is needed for these sessions. The OSCE/ODIHR report noted that the use of an NDA seems to "limit the observers' ability to comment on the source code and, therefore, transparency of the system" (OSCE/ODIHR 2011: 14).

Secrecy and Freedom of the Vote

After the end of voting the "envelopes" with personal data are separated from the votes themselves and the latter are transferred to an isolated computer in order to carry out the final tally. This computer is protected by a collegiate digital signature owned by Estonia's National Electoral Commission (NEC).

Given that freedom and secrecy are key challenges with voting from an unsupervised environment, voters are able to revoke their votes and cast them again through the Internet or even with paper ballots during the advanced election period. Regarding the secrecy of the vote, Estonian literature splits this principle in two sub-rules: the private proceeding of voting and the anonymity of the vote. The latter is guaranteed by the computer application itself and the former "is required to ensure free voting

[but] ... is not an objective *per se*. Consequently, instruments aimed at securing secrecy can be adapted, provided that voters are given the opportunity to vote freely for their preferred party without fearing condemnation or expecting moral approval or material reward." (Madise and Vinkel 2010: 62) Therefore, this second understanding of secrecy is directly linked to the freedom of the vote and to solutions already mentioned to guarantee it, that is to say, the revocation of votes both by electronic and paper means.

Accessibility of Internet Voting

In terms of the identification of voters, the Estonian solution is based on an ID card that is deployed nationwide and also used for other purposes. As of January 2011, more than 1.1 million people (almost 90 percent of the population) had such a card. To vote, citizens are issued two passcodes to be used with the card. Authentication requires a card reader, but these are easy to buy and widely available on computers in public spaces such as public libraries and Internet cafes.

The card is a chipped picture ID token using the standard state supported X.509 public key infrastructure. It allows for secure remote authentication and legally binding digital signatures. In 2007, Estonia introduced a mobile-ID system where a mobile phone can be used as ID card and card reader at the same time. It offers the same functionality in terms of authentication and digital signature as the regular ID. While the X509 norm may be seen as weak in terms of authentication, the move towards mobile ID introduces a second communication channel and a greater level of security. However, less than 2 percent of voters used the mobile ID option in the 2011 parliamentary election (OSCE/ODIHR 2011: 11).

The Estonian Internet voting application supports Windows XP SP 3, Windows Vista and Windows 7, Linux (Debian 5.0, openSUSE 11.3, Ubuntu 10, Fedora 14) and Mac OS X 10.4 Tiger, 10.5 Leopard, 10.6 Snow Leopard, combined with the most common browsers. The choice of supported configurations was made based on the most commonly used platforms in the county. In 2008, when refurbishing its Internet voting application, Estonia had to choose between a standalone downloadable application and a "Java" based solution running within the web-browser. While the latter is more convenient to use, the former is considered more secure. The choice was made to develop the downloadable standalone solution.

Finally, during the March 2011 parliamentary election, the helpline (both phone and e-mail) received a total of 1,418 contacts, which represents 1 percent of the total number of e-voters. The main issues raised were the setup and use of the ID card, connection problems with the voting client and problems linked to the setup of the Mobile ID solution.

The Role of Stakeholders

Taking into account that the Estonian Internet voting project was born within a broader national e-strategy, public authorities assumed a key position in the development and implementation of this new voting channel. This role has been compatible with the involvement of external managers and suppliers, like Cybernetica - a private firm that has always been the provider of the Internet solution.

Following the conclusions of the assessment mission deployed by the OSCE, the distributions of tasks among such stakeholders has raised some concerns given that the electoral commission does not have sufficient in-house IT expertise and therefore has to rely on the IT department of the Estonian Parliament, which also hired an external project manager for Internet voting. Moreover, most people remain involved during consecutive elections and create "an environment where critical questions were no longer asked and where detailed protocols of proceedings were too rarely part of the process" (OSCE/ODIHR 2011: 9).

Estonia has not involved average voters in the *interface* development process. However, associations representing visually impaired people were involved in finding the best support for on-screen readers. Public "mock" demo elections are held prior to all "real" elections.

Regarding political parties, Estonia provides clear evidence that the democratic challenges generated by Internet voting may not arise to the extent theoretically expected among such entities. Except for the last elections in 2011, political parties rarely participated in the testing and training sessions provided by the electoral authorities. There appears to have been little social concern on this issue, political parties seem to have confidence in the electoral authorities to the point they did not consider it useful to attend such sessions;

> *"no political parties exercised their right to have access to the process and to observe the setup procedures, nor did NGOs or civic associations attempt to observe the process in a comprehensive manner. Although the NEC organized a short training course on the system and invited political parties and the public to attend, only two persons completed the course"* (OSCE/ODIHR 2007: 19)

Furthermore, no significant NGOs have been created in Estonia to conduct the oversight tasks that other associations carry out in France, Belgium or in the U.S..

As mentioned earlier in this report, the 2011 election changed this scenario. Paavo Pihelgas, an IT expert, submitted a complaint aiming to cancel the Internet voting system (Simons 2011) and the Tallinn City Council also filed a motion with Supreme Court with a similar purpose (Rikken 2011). While the cases were rejected, a parliamentary Internet voting committee was subsequently created in order to evaluate the system and suggest potential improvements.

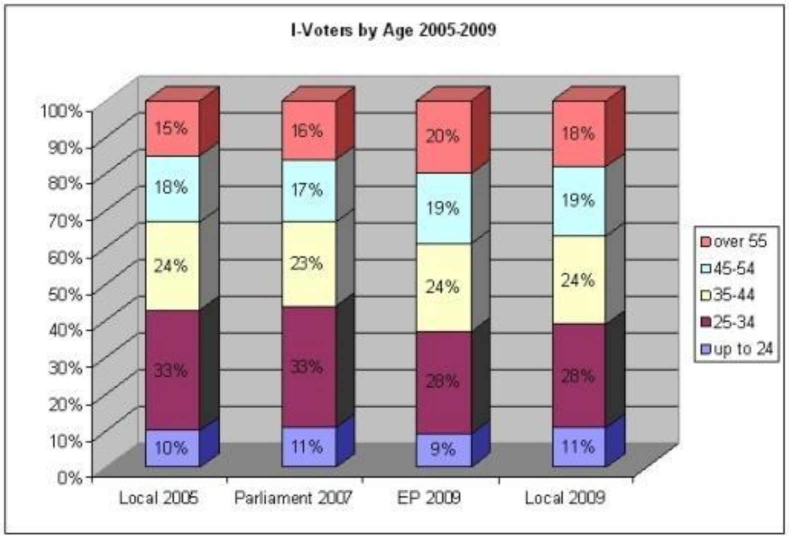
Statistical Data

Key data related to the use of Internet voting is provided in figure 11 above. Electoral authorities also commissioned a group of experts to research the use of Internet voting in Estonia, and key research findings are presented below in figures 12 and 13. After several surveys the researchers concluded in 2011 that, although some inequalities in Internet voting usage exist, based on age and gender, these inequalities are losing influence as people "grow into e-voting" (Trechsel 2011: 21).

However, the linguistic dimensions of Internet voting still generate great concerns (see Figure 14). Linguistic minorities make up 32 percent of the total population but, "on average only 3.3 percent of the e-voters are Russian (or other)-speaking [i.e. non-native Estonian speakers]" (Trechsel and Vassil 2010:

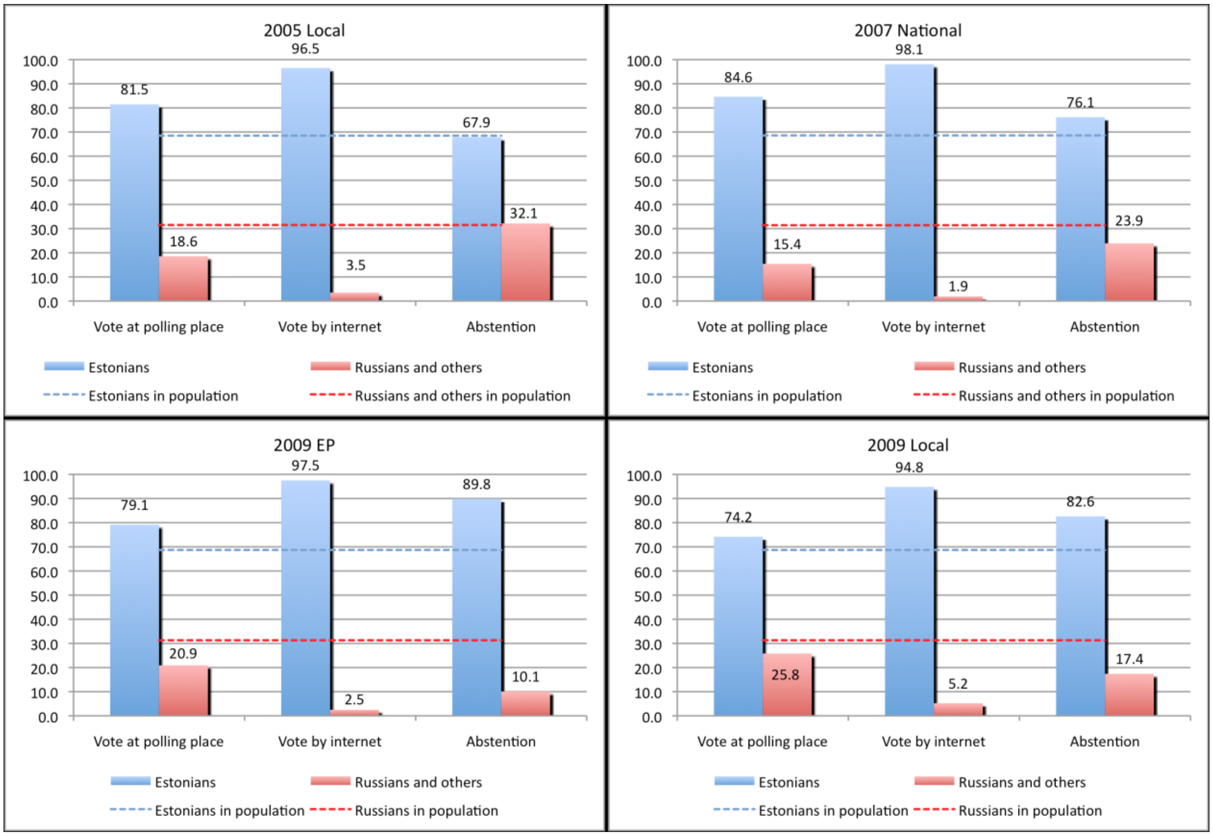
45). Beyond the reasons linked to the political socialization of such groups, it should be noted that the Internet voting project has only been deployed in Estonian. Although national electoral authorities make some efforts, in 2009 “the voting system remained ‘Estonian-only,’ which might have induced most Russian native speakers not to use this channel of electoral participation.” (Trechsel and Vassil 2010: 46).

Figure 12 - Internet voters by age 2005-2009



Source: (Madise and Vinkel 2010: 66)

Figure 13 – Language Groups By Voting Type



Source – (Trechsel and Vassil 2010: 46)

France

For three elections (2003, 2006 and 2009), French citizens living abroad have been able to elect, by Internet, the 155-member consultative Assembly of French Citizens Living Abroad (AFE, *Assemblée des Français de l'étranger*). This body elects the 12 senators (out of 348) who represent the 1.5 million French expatriates in the upper house.[111]

In 2012, French expatriates will be able for the first time to elect eleven members of the parliament, using Internet voting, postal voting, and proxy voting or by visiting a polling station in France. Internet voting is only allowed for elections where postal voting is also permitted. Due to a lack of data from 2003 and 2006, this case study will consider only the 2009 online vote, at least as far as the technical details are concerned.

Assembly of French Citizens Living Abroad

French citizens living abroad obtained political representation in the 1946 Constitution, in recognition of their contribution to the fight for the liberation of France from Nazism. In a rare institutional construction they received seats in the Senate, which represents the provinces, rather than in the lower house, which represents the people.

Initially, the representative associations of French expatriates elected the senators representing the French abroad. In 1948, a decree created the Superior Council of French Citizens Abroad (CSFE). In 1982, a law instituted its election by direct suffrage of the expatriates. In 2004, the CSFE became the AFE.

Elections for the AFE take place every three years, alternatively held in Europe, Asia and the Middle East (2003 and 2009 as far as Internet voting is concerned) at one time, and in the Americas and Africa (2006), at one time. This means that that the assembly is renewed by half every three years.

Two electoral rules apply, depending on the number of seats allocated to the different constituencies. Both are single round elections. In constituencies where there are no more than two seats to be filled, the election is a majority vote, and voters can mix candidates from different lists. In constituencies where there are three or more seats to be filled, the election is proportional and it is not possible to vote for candidates from different lists.

Elections for the AFE were due in the first zone in 2012, but will be postponed until 2013 and the current legislature will be extended by one year. In 2012 French expatriates will be able, for the first time, to participate in the parliamentary election. A constitutional change adopted in 2008 gives them 11 directly elected representatives in the lower house. In addition, there is a presidential election[112] that same year (without Internet voting). Both elections are majoritarian, with a second round if necessary. It has been deemed wise not to organize a third election the same year. This does not threaten the AFE existence.

The rationale for Internet voting

Elections for French residents are organized by the Ministry of the Interior and elections for French expatriates abroad are organized by the Ministry of Foreign Affairs. In the early 2000's, the Ministry of

[111] All senators are designated by indirect election, not only those representing French abroad.

[112] In 1976, French expatriates obtained the right to vote for presidential elections and referendums.

Interior began to cautiously introduce voting machines in polling stations in France. Although there has not been any coordination between both Ministries on the issue, Internet voting for French abroad was a variation of a domestic policy that was pursued.

The Ministry of Foreign Affairs was trying to reach out to the growing community of expatriates using new technologies. It created an e-Gov portal that was scarcely known among its target public, not least because there were very few available online transactions for this community. The dwindling network of French consulates, which function as polling stations, called for some kind of additional measures to ensure political rights for expatriates. Casting a ballot for the presidential election and for referendums has to be done at the consulates. The use of information and communication technologies to enable French expatriates to vote was considered a “quick win” – to use IT jargon – at low cost.[113]

In France, Internet voting is not limited to the AFE elections. It is widely used for all types of private elections and semi-official ones such as labor courts, trade unions representatives in different official instances, chambers of commerce or the Bar council. The prevailing idea behind this wide use of online voting is increasing turnout by simplifying ballot access.

Current situation

Originally, the use of Internet voting by French expatriates was seen as an ad hoc situation that did not require a long-term approach. The online component of the 2003 and 2006 AFE elections was organized by private providers with no prior experience with political elections. In 2006, however, the provider was selected following a call for tender.

After a new call for tender in 2008, the French Ministry of Foreign Affairs bought a permanent license for Pnyx, the Internet voting solution by Scytl. By law, the server must be located in France. The Ministry may organize an unlimited number of ballots on the system with Scytl as the service provider for the system. Scytl ran the 2009 AFE election, which was hosted by Athos Origin, and will run the 2012 parliamentary election.

The long-term stance adopted by the Ministry marks a change in its approach to Internet voting. This was first seen as an extension of postal voting, as indicated by the wording *vote par correspondance électronique* (vote by electronic post) used up to 2009 in all legal texts. Since 2009, the wording was changed in most cases to refer to “electronic voting.”

The growing requirements of the CNIL (National Commission on IT and Freedom for *Commission nationale informatique et liberté,* the body charged with enforcing privacy protection) and the increased political rights of French expatriates also played a role in the decision to organize a tender allowing the Ministry to contract a system for an unlimited period of time. For a long-term approach to Internet voting for political elections to prevail, a process of “industrialization” of Internet voting must take place and the legal framework must somehow be simplified.

[113] According to a document of the Assembly of French citizens living abroad, the online ballot in 2003 cost only 61,000 euro. In 2006, it cost 2 million euro – see Seingry (2008: 22) and http://www.expatries.senat.fr/intervention_del_picchia.html [last accessed February 29, 2012].

Eligible Voters and Internet Voting Turnout

As elections to the AFE are held alternatively in the two world zones, only half of the French abroad can vote at the same time. In 2003, for its first use, access to Internet voting was limited to the some 50,000 registered French citizens living in the USA and Canada.

In 2006, the some 525,000 French expatriates living in Asia, Europe and the Middle East could vote online. In 2009, the 340,000 registered French citizens living in Africa, North and Latin America could vote online. In both of these cases, they had to register with their consulate in advance.

Figure 14 – French Internet Voting Statistics[114]

Election Year	Region	Potential Eligible Voters	Registered Voters	Number of Votes Cast Online	Share of total votes cast online
2003	North America	50,000	n/a	4,384	60.6%
2006	Asia, Europe, Middle East	525,000	28,000	10,201	14%
2009	Africa, North America, Latin America	340,000	n/a	6,026	9%

Alternative Voter Channels

In addition to Internet voting, French expatriates may participate in AFE elections through advanced postal voting and at polling stations on ballot day in embassies and consulates.

Period of Internet Voting

The period of Internet voting has varied in 2003, 2006 and 2009, with periods of 12, 6, and 15 days respectively in advance of voting at polling stations. Internet voting was possible from May 19 – 31, 2003 (polling stations opened on June 1) from June 6 – 12, 2006 (polling stations opened on June 18) and from May 20 - June 4, 2009 (polling stations opened on June 7). This changing pattern appears to be a trial and error process in search of the appropriate format. It also indicates that there is no legal regulation regarding the Internet voting opening period, bar that it must be finished before polling stations open.

Voter Identification and Authentication Mechanisms

The 2003 voting system

In 2003, voters received a code and a password enabling them to identify themselves on the voting web site by post from the administration.

[114] 2003 data from http://test.edri.org/edrigram/number4.16/evotingfrance; 2006 data from http://www.expatries.senat.fr/intervention_del_picchia.html, http://www.strategie.gouv.fr/content/note-de-veille-n°-36-lundi-27-novembre-2006-analyse-le-vote-electronique-entre-utopie-et-rea#les-ressources and www.edri.org/edrigram/number4.16/evotingfrance; 2009 data from http://www.assemblee-afe.fr/elections-des-conseillers-a-l-afe.html [all last accessed February 29, 2012].

The 2006 voting system

In 2006, voters had to register with their consulate to vote online. To do so, they had to send an email or a letter, after which they received a password to access the Internet voting site.

The 2009 voting system

In 2009, citizens had to create their own password on the French eGovernment platform GAEL (Guichet d'Administration Electronique). This was expected to attract many new users to this platform. To create an account, citizens had to log on to GAEL using their consular identification number (NUMIC), name, birthdate and passport number. To vote, they would use their NUMIC and the eight to 12 alphanumerical character-long single use password they had created.

The authentication for the voting transaction itself took place on Pnyx, the voting application from Scytl, using the NUMIC and password voters had created on GAEL. This was only used to create the password. In 2006 and 2009, citizens did not need to go to a counter and provide proof of identity. For this reason, the authentication on the Internet voting web site is considered weak. When the voter connects to the voting web site, a Java applet is downloaded to the personal computer. For the AFE election, the applet size had been reduced as much as possible to fit the low bandwidth used to access Internet in Africa and parts of South America.

The voter is known to the system by his NUMIC only. The NUMIC is encrypted by the Java applet in the voter PC and the system only contains encrypted NUMICs. The vote is similarly encrypted on the voter PC and digitally signed with an individual signature. At the end of the voting transaction, voters received an individual code to confirm their vote. This code did not confirm the value of the vote, but only the fact that the vote had reached the ballot box. After the ballot counting, the codes corresponding to all counted ballots were published on the Internet, allowing voters to verify that their vote had been counted.

To prevent multiple votes by the same voter, a manual procedure has been adopted. Internet voting closes on Thursday before Election Day, after which the list of citizens having voted is established and sent to the consulates. This list is compared with the postal votes received to detect possible duplicates, and citizens having voted by post are then added to the list. Finally, on Sunday, Election Day, there is a complete list of who has voted.

Legal Basis for Internet Voting and Challenges

French expatriates may vote in municipal, cantonal (a subset of the departments), regional, European and presidential elections (and, as of 2012, in parliamentary ones). Historically, for the AFE elections, they have been able to vote by post or in person at consulates and embassies. For the other elections, they could only vote in France or by designating a proxy in France. Their right to vote remotely is an exception to the common legal framework, as postal voting for political election has been abolished in France since 1975.

The last 20 years have roughly coincided with a growing number of French expatriates[115] and an increased consciousness of their rights. Recommendation R(86) 8, adopted in 1986 by the Committee of Ministers of the Council of Europe, encourages the Council's member states to grant their expatriates political rights. While in France the strong symbolism of people attending the polling station is an important value,[116] it struck the lawmakers that expatriates were having significant difficulties in participating in this traditional manner. The very low turnout in the AFE election[117] was a strong signal.

One cannot help being struck by the range of legal instruments regarding the political rights of the French abroad and the implementation of Internet voting. No less than one Council of Europe convention (Nr 108 on individual protection against mechanized data treatment), one directive from the European Parliament (95/46/CD, on the same topic), five national laws, seven decrees, two government decisions and two deliberations are quoted in the documents dealing with the 2009 election of the Assembly of French Citizens Abroad.

There are in fact two families of legal norms ruling Internet voting in the case of the French abroad. One deals with the protection of privacy – very strong in France – in a context of mechanized data treatment, and the other relates to political rights. The main document of the first family is the CNIL "deliberation." CNIL has been created by a law known as "IT and freedom" (*informatique et liberté*), to supervise the law's implementation, publish recommendations to make it operative and has also an educational role for the public.

The CNIL published in 2003 a "declaration" (a set of compulsory rules) on electronic voting,[118] which it has rewritten in 2010.[119] It states, among other provisions, that the system must comply with the General Security Referential[120] (RGS, *Référentiel general de sécurité*), a set of IT security rules and good practices that French public administrations must implement. A National Agency for the Security of IT Systems (ANSSI, *Agence nationale de la sécurité des systèmes d'information*) has been established to supervise RGS compliance. Adopted in 2010, the RGS is included in the specifications for the 2012 election. The legal procedure also imposes the Ministry of Foreign Affairs to ask the State Council (*Conseil d'Etat*, the highest administrative authority in France) its opinion on the compliance of the Internet voting solution with the CNIL declaration.

The second family of norms is mainly enshrined in the French Constitution and the electoral code. A law adopted in 2003 allows Internet voting for the AFE election in a single line of text. All further provisions, and notably all the ones regarding ballot organization, roles and responsibilities of the Ministry, the AFE, the electoral bureau and solution provider, are regulated by a government decree. A new decree is issued for each ballot. There is no obligation whatsoever to publish any details about the system,

[115] The number of French citizens abroad has grown from 900,000 registered units in 1995 to 1.5 million as of 31 December 2010. It is estimated that another 500,000 are not registered, putting the total at 2 million.

[116] The importance of the vote is underlined by the compulsory presence of a policeman at the entrance of each polling station.

[117] The turnout for AFE elections was 28.17 percent in 1994; 24.08 percent in 1997; 18.97 percent in 2000; 21.82 percent in 2003; 14.25 percent in 2006 and 19 percent in 2009.

[118] See www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/12/ [last accessed February 29, 2012].

[119] See www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/249/ [last accessed February 29, 2012].

[120] See http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/ [last accessed February 29, 2012]. There is an English version of the web site.

however. Only the Ministry, the CNIL, AFE and to a lesser extent political parties and the candidates, can access technical information and audits.

Law mandates the order in which candidates and political parties are displayed on the screen. The parties' lists are displayed according to their registration order. The list that registered first with the authorities is displayed first and the list that registered last is displayed last.

Electoral bureau

The main change over time in the legal regulation regarding Internet voting concerns the composition of the Electoral Bureau, which is ruled by government decree. This bureau is the owner of the votes, as it owns the ballot box encryption keys. In 2003, there was no other specific instruction in the decree regarding the bureau's task. In 2006 and 2009, it was also responsible for the respect of the procedures surrounding the voting process.

In 2003, the bureau comprised of one representative of the Ministry, one of the AFE and one of each list competing in the election. In 2006 and 2009, it was made of the secretary general of the AFE, at least four assessors, but at most eight, and their substitutes designated by the AFE and a secretary designated by the Minister of Foreign Affairs. A technical committee assists the bureau.

The responsibilities of the bureau in the framework of Internet voting were the following:

- Checking that security measures aimed at preserving the vote secrecy,[121] the integrity of votes, the confidentiality of the voters' register and that clear separation from the electronic ballot box are respected
- Deciding on the measures to be taken should an emergency affect the election process (contingency plan)
- Owning the ballot box decryption key
- Ensuring that the electronic ballot box is empty before the beginning of the election
- At the end of the election, before counting the ballots, checking the system's integrity

This structure was problematic in that the bureau's members were given a responsibility for which they had no technical competency. They had to trust the technical committee, which they did not choose, while endorsing important responsibilities.

In 2012, the electoral bureau will be made up of a member of the State Council, the Director of the Consular Affairs at the Ministry for Foreign Affairs, the Director of Modernization at the Interior Ministry, the Director of the ANSSI and three members of the AFE with their substitutes, elected by their peers. The bureau's responsibilities are unchanged. The change in the bureau's composition expresses a will for greater professionalism in the oversight of Internet voting.

The 2006, 2009 and 2012 decrees foresaw the possibility for the Ministry of Foreign Affairs to draft a list of countries from which Internet voting would be forbidden for security reasons. This provision has

[121] In 2006, there was only one vote cast in Afghanistan. To protect the voter's identity, his vote was not decrypted by the Electoral bureau, but by a court usher, upon decision by the bureau.

never been used so far, but it is still under discussion for 2012. It seems that French authorities fear offending a foreign country by drafting either a white list or black list of countries.

Trust in Internet Voting

The law allows political parties and candidates to mandate an expert to observe the online part of the AFE elections. In 2006, three experts observed the Internet vote. They published reports whose common characteristic is to underline the impossibility of observing whether the system works properly (Pellegrini 2006, Lang 2006, Appel 2006). Only the respect of the mandated procedures can be verified. These reports had no consequence and were ignored by the AFE, the parties and the candidates having mandated the experts.

In France, activists grouped around the association called *Ordinateurs de vote* (vote computers) are fighting voting machines. They did not fight Internet voting much,[122] probably because the stakes were low with the AFE and because the CNIL declaration stands as a significant obstacle to Internet voting for political elections for French residents.

The CNIL recommendation of 2010 imposes a series of tests and audits to the system. This resolution mandates that every electronic voting system be submitted to independent expertise covering software and hardware, the use of the system during the ballot period, the ballot counting and the handling of the records of the ballot. This entails auditing the source code, auditing the cryptography, auditing the servers and their architecture, and auditing the network.

The expert who will perform these audits is chosen by the ballot organizer (the AFE). They must:

- Be an IT security specialist
- Not have any financial interest in the company that provides the eVoting solution or in the organizer of the election (here, the AFE)
- Have analyzed at least two similar systems in the past
- Have followed the CNIL workshop on electronic voting

Any change in the system must be assessed anew by the expert. The expert's reports are given to the ballot organizer and the CNIL, but are not made public. The expert must provide a technical means to ensure ex-post that the software used for the ballot has not been altered since it was first analyzed before the election.

The system must be able to provide the following confirmations after the election:

- Encryption has not been tampered with during the election
- Encryption keys are only known to their owner
- Votes are fully anonymous
- List of voters having voted are published after every election only contains people who actually cast a vote (see the section on Secrecy protection mechanisms below)

[122] At least not in France, but they wrote to the Geneva government and parliament to try blocking internet voting in Geneva.

- The ballot box that has been decrypted is the actual ballot box; it does not have any other content than the votes
- No partial ballot counting could have been performed during the election
- The electronic ballots counting can be repeated

Secrecy and Freedom of the Vote

The State apparatus is divided on Internet voting. The CNIL distances itself from electronic voting in the preamble of its 2010 declaration on the topic. After recalling the principle of a free and secret vote, the CNIL writes that the audits it conducted since 2003 have shown that the existing voting systems did not provide all the required guarantees. Hence, the CNIL "is reserved as far as the use of electronic voting devices in the framework of political elections."[123]

The CNIL 2009 annual report (CNIL 2009), covering the year of the last AFE election to-date, explains that no online ballot it supervised in 2009 was fully compliant with the CNIL declaration. CNIL controls have evidenced the "insufficient guarantees" offered by voting systems in terms of security and data confidentiality in respect to the legal requirements. These requirements are very exacting and are contested within the State.

According to French electoral law, the list of all citizens having voted must be published right after every election. Extracting this data from an electronic system might compromise the anonymity of digitally signed votes. It is, therefore, almost impossible not to breach CNIL rules for political elections.[124]

In 2009, the CNIL forbade that the voters using Internet to cast their ballot be redirected after the end of their voting session to an online questionnaire. This prevented gathering any information on the socio-political profile of Internet voting users.

The Accessibility of Internet Voting

Accessibility, understood as lowering the access threshold to the voting procedure for disabled or elderly citizens, was not a priority of the French approach. The objective of Internet voting was clearly to provide a modern remote voting channel in order to increase turnout among "regular" registered citizens.

This explains why the W3C norms were not considered in any of the three elections to-date for the AFE. For the 2012 parliamentary election for French abroad, the State has added compliance with W3C norms to its requests.

In 2009, Extelia, the French company that was Scytl's partner for that year's election, organized focus groups together with the AFE to test the usability of the voting interface. These groups were composed of members of the Senate and of the AFE. Only marginal changes were done to the interface after these

[123] See the November 26 2010 press release announcing the new declaration at www.cnil.fr/la-cnil/expertise/actualite-expertise/article/la-cnil-met-a-jour-la-recommandation-vote-electronique-pour-la-rendre-plus-pragmatique/ [last accessed February 29, 2012].

[124] The CNIL wants the system to give voters an anonymous token to maintain the anonymity of the vote, while being able to produce the list of those who have voted. For the Ministry, anonymous token would prevent any control on the eligibility to vote of those casting a ballot.

tests.[125] Scytl worked however to reduce the size of the java applet that its system uses to allow voters in South America and Africa to vote using dial up Internet connections. The web site had been developed in French and English, but only the French version was put in production, as the Ministry did not know how to justify the use of a foreign language on an official voting web site.

In 2009, all standard combinations of the most common browsers with Windows, Mac OS and Linux were supported. As the helpdesk was managed at the embassy level and no consolidation of the queries has been done, it is impossible to have detailed data on the difficulties voters have encountered. There is also no data on the 2003 and 2006 operations.

The Role of Stakeholders

The stakeholders have had little to say either in the decision to implement Internet voting or in its development. Although the initial impulse came from Senators, the Ministry of Foreign Affairs and the administration have run the project largely in isolation after the Senate's and the National Assembly's approval for the project. Even the AFE, whose members were to be elected online, have had little to say about Internet voting.

Although candidates and political parties may observe the elections, only in 2006 did observers attend the process (see previous discussion). And although their reports contained criticism of the absence of transparency of the Internet voting system, no-one nominated representatives in 2009. French domestic public opinion may not even be aware that France is using Internet voting in political elections, as it is limited to expatriates. Opposition to electronic voting, whether to the voting machines used in some French municipalities or to Internet voting as used in private and semi-official elections, has never received widespread public support.

Finally, the mock elections organized in 2009 and 2012 to test the system's interface are almost the only opportunity for stakeholder involvement in the process of Internet voting. No surveys of domestic or expatriate opinions about the use of Internet voting in France are known to have taken place.

[125] Phone interview with Jean Souto, head of French projects for Scytl, October 20, 2011.

Switzerland–Geneva

Switzerland's institutions embody the concepts of direct democracy and federalism. It is the latter that gives each canton broad autonomy in the way they implement their political rights. Regarding Internet voting, there are for instance three different systems used in three Cantons in Switzerland. This study focuses on the Geneva system, the longest serving one and the only one to have been updated since its development.

In 2000 the Swiss federal government launched the Internet voting project, arguing that "by implementing electronic voting, Switzerland could (…) play a forerunner role and show the community of nations (…) that IT science can help them too in introducing elements of direct democracy."[126]

The fact that Swiss voters are faced with four to six ballots a year created a desire to increase accessibility. The success of postal voting and its impact on turnout also generated a desire to further develop remote voting channels.[127] Other factors include the high level of Internet penetration; the fact that 10 percent of Swiss citizens live outside of the country, but only two percent were registered to vote from abroad; low turnout among Swiss voters under the age of 40; and high support for Internet voting, measured through public opinion surveys.[128]

Ultimately, however, Internet voting was introduced as a means to increase voter turnout, which has been decreasing over the 20th century. This was a trend that even the introduction of women's suffrage failed to reverse.[129] Studies by the GFS, a Bern polling institute,[130] which conducts electoral studies on behalf of the federal government, show that for referendums and initiatives, the driver of citizens' participation is their having a direct stake in and understanding the issues on the ballot.[131] This "tailor-made" participation could partly explain why turnout for elections is low in Switzerland compared to European comparisons.[132]

The Internet voting project has four phases:

- Offering citizens the possibility to vote online for referendums and initiatives
- Offering citizens the possibility to elect representatives online
- Offering citizens the possibility to digitally sign referendum and initiative forms
- Offering political parties the possibility to digitally sign candidates' lists

[126] www.admin.ch/ch/f/ff/2002/612.pdf [last accessed February 29, 2012].

[127] Generalized postal voting was authorized by federal law in 1994. Geneva was one of the first cantons to implement it in 1995. As a consequence, turnout rose by 20 percentage points between 1995 and 2003, reaching an average of 55 percent for referendums and initiatives and 45 percent for elections. Nationwide, the turnout gain amounted to five to seven percentage points.

[128] Such as the eGov Trendbarometer of the Bern School of Applied Science, which is no longer available online.

[129] Vaud and Geneva were first to grant women the voting right, in 1959. In 1970, women got the voting right at the federal level. In all cases, this development took place after a popular vote.

[130] See for example http://www.polittrends.ch/vox-analysen/daten.php [last accessed February 29, 2012].

[131] Turnout is lower for elections than for referendum or initiative ballots. Switzerland never mixes elections and referendums or initiatives in a same voting operation.

[132] Swiss residents are automatically registered as voters, which biases comparisons with countries where voters must actively register. Expatriates have to register.

At the end of 2011, Switzerland was at the beginning of phase two. There is no timetable for the succession of phases and the federal government has on different occasions communicated different terms regarding the time when Internet voting would be accessible to all Swiss voters.

For Internet voting, the Swiss Confederation developed a centralized management structure that allowed it to retain control of the project. In 2000, it signed an agreement with three cantons (Geneva, Zurich and Neuchâtel) who volunteered to implement Internet voting. In return for Confederation funding (80 percent of their development costs up to the year 2005), these cantons agreed to develop an Internet voting system and make it available to any of the 23 remaining cantons free of charge.[133] The Confederation would retain management of the project for an unspecified duration.

After 22,000 Swiss expatriates were able to participate online in the federal election in October 2011, the Confederation said that for the next election in 2015 a majority of expatriates should be able to vote online. This leaves open the question of the Internet voting for residents: in 2015 the Internet voting project will be 15 years old. The Confederation limits Internet voting to Swiss citizens living in the European Union or in a country that has ratified the Wassenaar Arrangement on trade and dual use goods and services.[134]

Geneva has a long history of integrating technology into the ballot counting process. In 2000, it was the only canton to have a computerized and centrally maintained voter registry. Furthermore, ballot counting for elections has been done by computers since 1961 and since 2000, ballots for referendums and initiatives have been counted by optical scanners.

In 2000, Geneva drafted a call for tender, which stated that the government would retain the intellectual property of any development done in relation with Internet voting. Hewlett Packard won the contract and started working in 2001, before losing interest in the project in 2004. Since then, all development has been done by the state IT department.

Geneva implemented Internet voting in a progressive manner. From January 2003 to June 2004, the system was used in five municipal referendums, first in villages of 1,200 to 3,000 registered voters, then in two cities of 9,000 voters. In autumn 2004, Internet voting was offered to all communes that had already used it (some 22,000 voters altogether) for two ballots containing both federal and cantonal referenda. A cantonal ballot for which 90,000 citizens could vote online took place in April 2005.

Until this date, Internet voting was conducted without specific parliamentary approval at the cantonal level, on the basis of a provision enabling the government to pilot new voting methods. In 2005, the Geneva government introduced a bill in parliament to give Internet voting a secure legal basis. No further online ballots were conducted until parliament passed the bill in 2008. The bill ended up being a constitutional amendment, knowing that the last word would reside with the voters, as with any change in the constitution.

[133] This means that any customization or knowledge transfer might be charged for.
[134] Dual-use goods or services have civilian and military use. Cryptography is a dual-use service.

Internet voting resumed in November 2008. In February 2009, by a 70.2 percent majority, Geneva voters accepted the constitutional amendment. This also created a permanent electoral commission, the CEC, whose mandate is to supervise all electoral operations and order any audit of the system it retains necessary.

Internet voting is currently available for all Geneva-registered voters living abroad and a small percentage of those living in Geneva. Geneva-registered voters living abroad can vote online provided they live in the European Union or in one of the countries that have ratified the Wassenaar agreement on the trade of dual-use (civilian and military) goods and services as cryptography can be considered as a military item.

On two occasions, in May and November 2011, all 240,000 Geneva citizens were offered the possibility to vote online, as these referendums were purely cantonal. This is however a rare occurrence. For the first time in October 2011, Internet voting was used in the federal elections. The Swiss expatriates voting in Basel could vote online on the Geneva system thanks to the hosting agreement between the two cantons.

Capping the use of Internet voting has had a limiting effect on its use. In Geneva, online turnout reached 22 to 25 percent of all votes cast before the introduction of the federal 20 percent cap. After the implementation of the cap, the share of online votes has fallen to 15 to 18 percent of all votes cast.

Internet voting has the same legal status as postal voting, in that both are classified as advanced voting channels. Advanced voting is possible for two weeks before Election Day for municipal and cantonal ballots and for three weeks before for federal ballots. If local and federal ballots are held together, (which is commonly done for cost-efficiency), then federal regulations apply. The period for casting an Internet vote closes at noon on the Saturday before the Sunday poll.

In order to cast a ballot, voters first type the voting web site URL in their browser, which creates a Secure Sockets Layer communication and the browser asks the website to present its electronic certificate. When voters type in their voting card number (the first step of the transaction), they activate the java applet. After accepting the legal notices, they fill out their ballot, check their vote and provide their personal information (password, date of birth and commune of origin) to validate it, before being transported to the page confirming the recording of their vote.

The voting card number is actually never exchanged: only an imprint of the number is sent out. This imprint is obtained by applying a cryptographic hash function to the voting card number. The system uses a correspondence table drawn up at the stage of the print files generation to determine the voting card number based on the imprint. From then on, the voting card number becomes a “shared” secret between the voter and the Internet voting system (Figure 15).

Figure 15 – Shared Secrets Used in Geneva Voting System

Shared secrets used for the vote	Source
Date of birth	Voter's personal data
Commune of origin	
Password	Electronic voting system (this is data reproduced on the voting card each voter receives home)
Voting card number	
Control code	

To finalize the transaction and send the vote to the ballot box, voters have to enter their date of birth and the password on their voting card, before selecting their commune of origin from a random list. The server checks the voter's personal data, checks that the voter is entitled to vote (no previous vote or vote via another method) then records their vote as follows:

- The vote and the voting location are encrypted with salt,[135] using the public encryption key for the ballot, and then recorded in the ballot box
- The voting card register is modified to record the fact that the voting card number associated with this citizen has voted
- The integrity meter in the database is decrypted, incremented and re-encrypted
- These three operations are carried out in a single database transaction in order to ensure that the filing of the vote meets the ACID requirements (Atomicity, Consistency, Isolation and Durability)

Swiss federal law sets a framework for federal ballots but allows discretion for cantons with regards to implementation. All ballots below the federal level – and they are the majority – fall under cantonal law. As a result, most aspects of electoral management vary from canton to canton, including the organization of the voters' registry (centralized or managed at communal level); the management of voters abroad (who may be a constituency of their own, spread among the canton's various municipalities or centralized in the capital city); the printing of the voting material (which may be printed by the canton, the municipalities or the districts – an intermediate organizational level between municipalities and canton); the management of the postal votes (which may be returned to the canton, the municipalities or the districts and which may or may not be counted on the Saturday prior to the opening of polling stations); and, the existence of third party ballot supervision.

In supporting three Internet voting systems, the Confederation thought it bought the certainty of being able to roll it out in all cantons, notwithstanding their differences. It was also argued that three systems would make it more difficult for hackers to nullify a nationwide ballot. At the time of this writing, eight years after the first eEnabled vote, progress in implementing Internet voting has been slow.

[135] Adding "salt" means adding random information (alphanumeric characters, for example) in a data chain before encrypting it. This is done to avoid that, once encrypted, similar votes (for example in a three questions referendum a "yes, yes, no" vote) look the same and could thus be recognized without having to be decrypted.

The federal law on political rights was amended to include online voting, but also to ensure a stronger degree of federal control than on the other ballot channels. Regulation of issues such as security or anonymity was not included into the law, but in a government decree that can be changed without parliamentary vote.

For federal ballots, cantons have to request the federal government approbation before offering Internet voting to their citizens. The government decree limits the possibility to vote online to 20 percent of the citizenship of any canton. This cap was calculated based on vote history with the following question in mind: should a problem occur, which share of votes can be lost without affecting the final result? The list of eligible Internet voters is determined after the canton proposes a list of select municipalities to the federal government for approval.

Geneva is going forward, having organized the largest number of eEnabled ballots in the country: 20 referendum or initiative ballots (that is together more than 100 proposals) and three administrative elections as of the end of 2011. The cantonal parliament has amended the law on political rights in October 2011 to authorize online political elections. The electronic voting system is continuously developed: a new version is released every year and security is constantly improved. As a result, no two ballots have taken place on the exact same platform.

At the cantonal level, as already mentioned, in February 2009 Geneva voters approved by a 70.2 percent majority a constitutional amendment that made Internet voting a regular ballot casting way for referendums and initiatives. In October 2011, the Geneva parliament amended the law on political rights to allow trial of Internet voting in elections. The first one will probably be the election of the Court of auditors (Cour des comptes) in September 2012, which is a majoritarian election.

There have been two legal cases against Internet voting. After the May 2009 referendum, when the introduction of biometric passports was accepted nationwide by a margin of 5,680 votes out of 1.9 million cast votes, several citizens in different cantons appealed to their cantonal government first and then to the Federal Court (the supreme court in Switzerland). They were opposing biometric passports and argued that such a close result should be considered an irregularity. They requested either a recount or the organization of a new ballot. The use of Internet voting was in their eyes an aggravating factor. The federal court dismissed the case for lack of evidence regarding the alleged irregularity and lack of legal basis to mandate a recount or a renewed ballot.

In May 2011, in Geneva, when for the first time all Geneva citizens could vote online, a citizen went to court to have the ballot annulled. He said that because of the inherent flaws of Internet voting, the outcome of the ballot could be the result of a massive fraud as well as a legitimate result. He didn’t bring any evidence in support of the fraud theory. The court dismissed his case on formal grounds (he did not introduce his case soon enough after having known that all Genevans could vote online in May 2011). He then appealed to the Federal Court, where the case is still pending. He repeated his attempt in November, arguing that Internet voting is inherently vulnerable and that the Geneva system does not offer the possibility to prove that the result of a ballot is not the product of a manipulation. The case is still pending at the cantonal court.

Trust in Internet Voting

A battery of tests is performed on the system before sealing it, to ensure that the system is working properly. These include predictive tests. The Internet voting system also integrates a series of controls that are activated during the ballot opening period:

- The CEC casts ballots in a dedicated ballot box within the system. It records its votes on paper. Before decrypting the Internet votes, this ballot box is decrypted and its content is compared with the paper records.
- An automated system automatically casts a vote every five minutes to check the system's availability. Should the system be down, an alarm would ring and alert an operator.

At the end of each ballot, when the results of the electronic votes are known, forensic statistical checks (square chi and Benford law test) are performed on the electronic vote total to see whether they are coherent with each constituency voting history. None of these tests are legally mandated.

The Geneva cantonal law mandates a triennial audit, which must be made public. The kind of audit (ISO certification, penetration test etc.) is however left to the decision of the administration. The first audit under this provision will be done in 2012. Its nature is not known yet. The public nature of its outcome restricts the type of audit; penetration tests can for example hardly be performed in this framework, as their results might be misused by the opponents to Internet voting and the media.

The Geneva system was developed before notions such as end-to-end verifiability or individual and personal verification had entered the public discourse on Internet voting. The system does not provide voters with the possibility to check whether their ballot has been cast as intended or counted as cast. This does not mean, however, that the system does not provide any guarantee. Right after casting their vote, users get a confirmation on their screen that their vote was received in the eBallot box. The system can display results in many different forms, including providing an image of each individual ballot. A stronger voter confirmation system is currently being studied.

Secrecy and Freedom of the Vote

The Geneva Internet voting system is based on the separation of duties and responsibilities between the stakeholders: the CEC, the administration, the police IT security officer, and the eVoting administrator.[136] The voter registry is fully anonymous and only contains voting card numbers and secrets shared between the system and the voter.

The system uses a double encryption of all data to protect vote secrecy and authenticity. The second encryption,[137] called the "secure channel" uses a mix of techniques: mutual SSL, data surencryption and message authentication. To manage these techniques, a java servlet is extended to the voter's PC and integrates with the browser.

[136] A detailed description can be found at www.ge.ch/evoting/english/doc/Flash_IT_vote_electronique_SIDP_final_english.pdf [last accessed February 29, 2012].

[137] The first encryption is based on the SSL protocol.

This approach, together with a sophisticated cryptographic scheme aimed at ensuring proper mutual authentication of messages, is also a consequence of using a single channel for the whole transaction and of not implementing a token at all. The secure channel supplements the absence of a second way of communication between the voter's PC and the voting server.

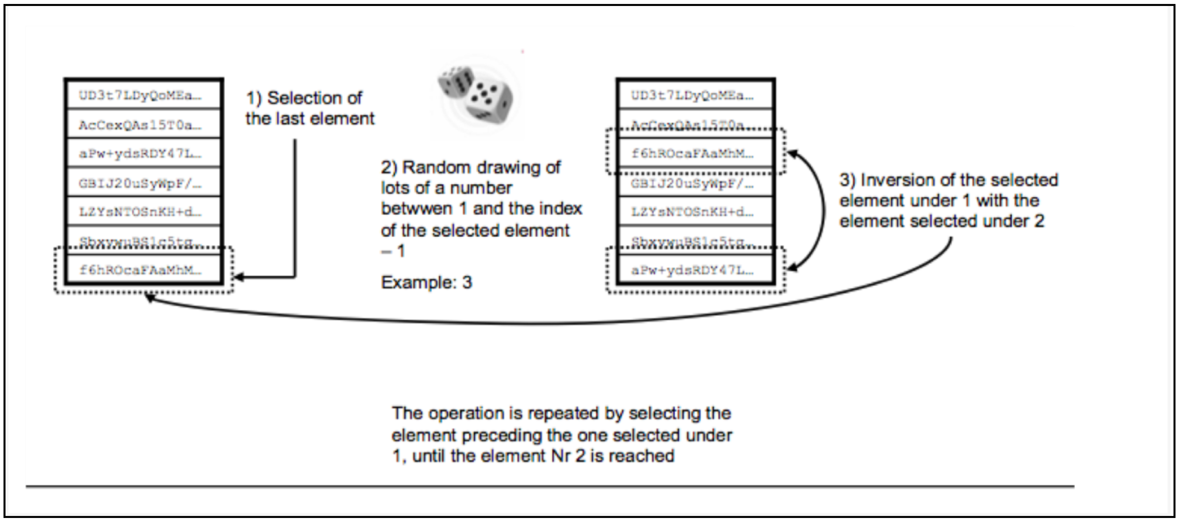
Authentication of the messages is ensured by adding an encrypted imprint to each one. The client calculates the imprint of the message and encrypts it with the private key associated with its electronic certificate. This encryption is based on an asymmetric key encryption algorithm. The server is protected by two keys owned by the CEC. To ensure that no invalid vote (or no damaging code) is inserted into the server, a validity check is performed before accepting any vote in the ballot box. Therefore, votes are briefly decrypted and re-encrypted before being allowed into the ballot box and the server has a chance to know them.

An encrypted integrity meter located in the server and activated only by the voting application prevents any insider to directly cast votes in the ballot box without being noticed. The system makes extensive use of JavaScript, which is vulnerable to a series of attacks. The system's source code is not signed, but the java servlet is.

Technical and organizational measures are implemented to prevent the establishment of a temporal link between a voter, for whom the vote casting time is recorded, and the encrypted vote, which is stored in the order of arrival. Encrypted votes are recorded in a database in their order of arrival, but are then subjected to a mixing process as follows:

- Before counting, all votes are uploaded into a memory compartment. Such uploading uses a specific function of the database enabling reading to take place in a random order
- This first structure is mixed using a quantum number generator. Figure 16 demonstrates the principle of this mixing
- Once the ballot box has been mixed twice, the application opens the collection of keys using as a password the combination of the two passwords with which the CEC has locked the ballot box.

Figure 16 – Geneva Ballot Mixing Process


UD3t7LDyQoMEa...
AcCexQAs15T0a...
aPw+ydsRDY47L...
GBIJ20uSyWpF/...
LZYsNTOSnKH+d...
SbxywuBS1c5tg...
f6hROcaFAaMhM...
1) Selection of the last element
2) Random drawing of lots of a number betwwen 1 and the index of the selected element – 1
Example: 3
UD3t7LDyQoMEa...
AcCexQAs15T0a...
f6hROcaFAaMhM...
GBIJ20uSyWpF/...
LZYsNTOSnKH+d...
SbxywuBS1c5tg...
aPw+ydsRDY47L...
3) Inversion of the selected element under 1 with the element selected under 2
The operation is repeated by selecting the element preceding the one selected under 1, until the element Nr 2 is reached

The Accessibility of Internet Voting

Geneva decided at the start of the project that Internet voting should be open to all. For each ballot citizens receive at home a single-use voting card, which carries some of the information they need to vote online. The information that is not reproduced on the card relates to the "shared secrets." This open-to-all procedure has one limitation - resident foreigners, who may vote on communal matters, have no municipality of origin. Their identification for online voting is therefore a bit less secure than for Swiss citizens.

In Geneva tests were conducted with voters and students. In 2002, a PC with the voting interface was installed in the waiting room of the service delivering passports. The public was invited to try the interface. A mock ballot was performed with high school students, to confirm the easiness of use of the system.

The Geneva voting web site is not totally compliant with the WCAG norms. A new release in the first half-year of 2012 should be compliant with the AA level of these norms. To achieve this, functions programmed with Javascript will be suppressed as the difficulty for disabled voters are related to the use of this programming language and to the lack of labels for the fields to be filled, such as the birth date field for voter authentication or the unfolding list of municipalities, where the voter has to chose his commune of origin in a list of 50.

The voting card also poses a problem for visually impaired voters. The password to be inserted into the voting web site is hidden behind a hologram which needs to be rubbed off. This is not done to protect the voter against vote theft, but to allow polling stations workers to see who might already have voted online, in order for them to check these particular voters' status (only one vote is allowed).

Switzerland has four official languages (German, French, Italian and Rumantsch) and it is a legal requirement to provide all of them for federal ballots. The voting web site is therefore offered in these four languages. The site also contains integrated tools to help voters. A clickable image of the voting card indicates where to look for the password or the site's certificate's fingerprint. A link opens a new window with the FAQs, the official explanatory brochure for referendums and to the political parties' vote recommendations. For elections, moving the mouse over the candidates' name will display a floating window with the information that the political parties print on the ballot papers (usually the age, commune of residence and profession of the candidates).

The Geneva systems supports Windows 2000, XP, Vista and Seven combined with a recent release of IE, Firefox, Chrome, Safari or Opera. For Mac OS X, the supported browsers are a recent release of Safari, Firefox, Chrome or Opera. For Linux (combined with Java Sun, Linux Java is unsupported), it takes a recent release of Firefox or Chrome to vote online.

The Role of Stakeholders

Political parties were at first very cautious about the use of Internet voting in Geneva. Today, only the Green Party and the nationalist Union Démocratique du Centre (UDC, in German SVP for Schweizerisches Volkspartei or Swiss People Party) still oppose Internet voting in Geneva (in most other cantons, the Greens support Internet voting).[138] The Geneva Green Party does not trust the system and fears an insider attack. The UDC is against remote voting in general and would also abolish postal voting. "Convenience voting" is not compatible with their idea of democracy.

The population as a whole supports Internet voting and trusts the administration. As an example, voter survey data indicates that 98 percent of Swiss nationals from Bern who voted from abroad in the May 15, 2011 election would vote via the Internet in the future (Canton of Berne 2011).[139] The initial pilot program did not include stakeholders such as political parties and civil society. This has largely been viewed as a mistake as it left no third party to endorse the system or the administration's choice vis-à-vis the activist and the media. This has resulted in great caution regarding giving access to sensitive information on the project (test reports, source code, etc.).

The legal possibility given to any Geneva citizen to see the source code has never been used. Only a handful of activists have tried to stop Internet voting, but they have had little support from the general public. A small group of IT people, most of them having worked on the project in the past and their ideas not having been considered the way they would have liked, has managed to convince a few member of the Geneva parliament belonging to the Green Party that the Geneva system was flawed. It is more a question of faith than of reason, as the MPs have no background in electoral matters nor in computer science and the statements of the disappointed IT people are not always related with the facts of the Geneva system. Yet, these stories can be popular in the media (ex-team members denouncing the system, for example) and many articles have been poorly supported by facts about the system. The issue is therefore not the risk of exposing flaws in the system, it is that media might use the reports in a manner not adequately supported by facts to discredit the Internet voting system.

[138] Survey data is available in the report "Das Potenzial der elektronischen Stimmabgabe." Schlussbericht Befragungen 2003/2004. Available at http://www.polittrends.ch/pub/vote-electronique.pdf [last accessed on January 11, 2012].

[139] See also (OSCE/ODIHR 2008: 20).

Annex 4 – Data Sheets: Non Remote Electronic Voting:

- Belgium
- Brazil
- France
- India
- Netherlands
- United States-State of Maryland

Data Sheet – Non Remote E-Voting
Belgium

Background	Belgium was an e-voting pioneer because it started using these devices in 1991. Long-term cost savings, a quick delivering of the results and the reduction of some organizational burdens were the main reasons alleged to back this initiative. Despite some criticisms, namely coming from IT activists (e.g. PourEVA), the overall e-voting project has not faced major problems, although there have been some critical scenarios like, for instance, the incidents in Shaerbeek and Jurbisse. Ticketing and ballot scanning were also piloted during these two decades. It is also worth noting the existence of specific independent bodies that supervise e-voting procedures. Federal and regional *Collèges des Experts* are appointed by the relevant parliamentary assemblies and issue a non-binding report after each election. In 2008, the Belgian government started looking into updating the current e-voting system, which was largely unchanged since the 1990s. A university consortium proposed up to five possible solutions with a specific recommendation to adopt a system that includes an e-booklet with a human readable part. In February 2011 the federal government, in conjunction with the Flemish region and Brussels, contracted Smartmatic to build a prototype that will match these features. The Walloon region decided in June 2010 not to use voting machines in 2012 and implement a voting pen method for 2014 elections.
Years of Use	1991 – 2011
Type of Elections/Referenda	All European, federal, regional and local elections since 1991.
Type of E-Voting System	A voting computer is used to help the voter cast his ballot, and the cast ballot is written onto a magnetic card which is then placed into an electronic ballot box, which reads the card (ballot) as it is inserted.
Brief Description of E-Voting System	The system is only available in those municipalities which decide to substitute paper means by voting machines. There are two systems certified by the government (Digivote and Jites). Both of them use up to three different electronic devices: a ballot box, a voting machine and a magnetic card. After being identified by traditional means, the voter receives a card in order to operate with the voting machine located into a voting booth. The voter selects his or her political options with the voting machine and they are recorded on the magnetic strip of the card. Meanwhile the ballot box remains in front of the polling board and, once finished with the operation with the voting machine, the voter has to insert his/her card into the ballot box that will read it. At the end of the Election Day, it will automatically carry out the final tabulation. Besides the voting procedures themselves, the electoral authorities also use electronic means, both to register the list of candidates, and for the final transmission and overall tabulation of results.
Status of the E-Voting Option	The system is currently being used, but the federal government expects to change the e-voting system in 2012 following the recommendations of the university consortium. Smartmatic has been selected to develop this new technical system. After being tested in 2011 and piloted in 2012, the government will adopt a final decision regarding the substitution of the current system. While the Flemish Region and Brussels share this initiative, the Walloon Region decided last June not to use voting

	machines in 2012 and will instead implement paper balloting for the 2014 elections.
Eligible Voters	All citizens in the regions deciding to implement the electronic voting technology.
Other Voting Channels Available	Proxy-voting, postal voting. Polling stations using voting machines do not allow paper ballots, except those coming by postal means.
Period of E-Voting	Only during Election Day.
Legal Basis for E-Voting	After being piloted in 1991 with a temporary legal basis, a parliamentary Act accepted in 1994 computerized voting methods. Beyond some procedural data, it also includes the technical features that voting machines have to comply with and the certification steps. In 1998, the Act has been changed to include the *Collège des Experts*.
E-Voting Usage	Currently, voting machines are being used by 44% of the population, but there is a clear bias comparing the different parts of the country. While 49% of Flemish voters are using voting machines, only 22% of voters in Walloon do the same. Brussels, meanwhile has completely substituted paper ballots with electronic machines.
Voter Identification Mechanisms	Voting machines do not change traditional identification procedures.
Audit Trail	Given that there are several voting booths in each polling station, a voter can verify in another voting machine whether his/her card has correctly recorded their vote's value. Ticketing was used once in 2003. The counties of Waarschoot and Verlaine included a paper-trail so that the voter could verify that the content of this receipt matched what they had previously selected with the voting machine. The experience was not successful and ticketing has not been used since. This is because tallying was significantly slower and the final paper and electronic results in Waarschoot did not match. Finally, it is worth noting that ballot's scanning was used since 1999 to 2003.
E-Voting System Provider	Steria / Solution “Digivote” Stesud / Solution “Jites”
Intellectual Property Rights of the E-Voting System	The Belgian Government retains the formal ownership of the e-voting system once licensed by two private suppliers.
Open/Closed Source Code	The source code is disclosed to: the entities that conduct the previous certification, the political parties (NB: without the cryptographic codes), the *Collège des Experts,* and the Ministry of Interior that also publishes it once the election is over.
System Testing and Certification Mechanisms	Each system is submitted to a previous certification that intends to verify whether it complies with the requirements included in legal regulations. Given that each election generates an upgrade of the e-voting system, the certification procedure should be repeated each time. Before opening the polling station, some “reference” votes are cast verifying afterwards that other voting machines correctly detect their value.
Transparency Mechanisms	Beyond the publication of the source code, key documents regarding the certification (e.g. certification reports) are not published, but the non-binding reports of the *Collège des Experts* are normally publicly released.

Court Cases Against the Use of E-Voting	In 2001, the *Conseil d'État*, federal supreme court, declared a local election in Jurbisse invalid due to inconsistent figures included in the final results that unveiled other procedural irregularities (CE arrêt nº 93716, 2nd March 2001 – A.98.896/VIII-2037). In 2007, the same court rejected another complaint based on procedural mistakes in Ixelles, but with no evidence of final incorrect results (CE arrêt nº 167711, 12th February 2007 – G./A.179.011/VI-17.299). Despite the fact that there have been no lawsuits, it is worth noting other cases with inconsistent figures that suggest problems in the voting and tallying machines. In 2004, the results coming from Antwerpen contained inconsistent figures regarding the European elections, but they have only been detected after being transmitted to the Federal authorities. Moreover, the European figures helped discover other mistakes in the regional elections that were held simultaneously. Inconsistent figures also helped to detect technical irregularities in Schaerbeek where, in 2003, one candidate obtained more preference votes than the list they were on. There also are legal complaints that challenge the overall e-voting procedure due to the lack of independent and external supervisors (CE arrêt nº 92957, 2nd February 2001 – A.98.167/VIII-1995) or to other generic reasons (CE arrêt nº 94526, April 4th 2001 – A.98.662/VIII-2015). Regarding the procedural transparency, the *Conseil d'État* also withdrew a governmental decision rejecting the disclosure of technical e-voting documentation (CE arrêt nº 95677, May 21st 2001 – A.77.331/XIII-513). The European Court of Human Rights (ECHR) decided in 2004 not to analyze three complaints because there were no evidences of breaches of the human rights protected by this Court (case nº 74247/01 — Mocole *et al.* v. Belgium). Besides the ECHR, the relevant internal bodies had previously rejected this case (CE arrêt nº 93325, February 16th 2001 – A.98.121/VIII-1992).
Key Reports/Documents	Official Electoral Website / Belgian Government - www.ibz.rrn.fgov.be/index.php?id=1622&L=0 Federal *Collège des Experts* / Reports - www.poureva.be/spip.php?rubrique19 Pour une Étique du Vote Automatisé (PourEVA) - www.poureva.be

Data Sheet – Non Remote E-Voting
Brazil

Introduction	Brazil is a federal republic where election administration is the sole responsibility of the federal state. Electoral fraud has been an endemic problem since the country's first parliamentary regime in the 1860s. The Tribunal Superior Electoral (Supreme Electoral Court or SEC) was created in 1930 after a rigged election triggered an outburst of violence. The SEC legislates, enforces legislation, runs elections and decides on legal challenges against ballots' results. The SEC has a central branch in Brasilia and regional branches in each province. In 1995, the SEC created a task force financed by the World Bank to find a way to stop fraud and strengthen political participation in a country where 30% of the population was illiterate. Electronic voting came up as the solution. SEC wrote the terms of reference for the system. The first eEnabled ballot was carried out in 1996, while the first nationwide all electronic ballot took place in 2000. Brazil claims to be the first country to have deployed electronic voting nationwide. Electronic voting succeeded with both reducing fraud and enfranchising illiterate voters. While the rate of invalid votes averaged 40% before electronic voting; it dropped to 7.6% in 2002. While electronic voting is a source of national pride and is widely trusted (97% according to a survey by the SEC), some academics, political parties and activists have called for greater transparency of the system. There is a nationwide ballot every two years in Brazil, alternatively for the federal parliament and the president and for the local and regional governments. The voting machines are called "electronic ballot boxes." We will use this terminology in this sheet.
Years of Use	1996, 1998, 2000, 2002, 2004, 2005, 2006, 2008 and 2010.
Type of Elections/Referenda	Local, regional and national elections as well as referendums (there were only 4 referendums in 48 years).
Type of E-Voting System	DRE with two numerical keyboards. The numerical keyboard has been chosen to evoke a phone keyboard, which illiterate people are familiar with.
Brief Description of E-Voting System	Simple, light and easily storable and transportable machine working on the electrical network, from its internal battery or a car battery. The machine has a triple function: • Voter identification • Vote recording • Vote tallying The machine totals the votes, but does not keep a representation of individual votes in the case of several races being organized the same day. The machine is made of two terminals, which have a numerical keyboard and a screen each: • One in the voting cabin for the voter to identify himself and cast his ballot • One for the electoral jury. Citizens who want to vote blank have to use a dedicated electronic ballot box called

	the "justification ballot box."
Status of the E-Voting Option	Currently used. It is the only method of casting ballots available throughout the country and in embassies for Brazilians abroad.
Eligible Voters	Voter registration is compulsory; as is voting from the age of 18 up to 70. Sanctions for not voting consist mainly of a restriction of one's rights: no public jobs are given to people who cannot demonstrate they have voted in the last election and no passports are issued to them, for example. Citizens aged 16 and 17 and those over 70, as well as illiterates are exempt from this obligation.
Other Voting Channels Available	None
Period of E-Voting	Election day, from 8 am to 5 pm.
Legal Basis for E-Voting	The electoral law. It is revised every second year to enact in law the electronic ballot box evolution and changing specifications.
E-Voting Usage	1996 (municipal and regional elections): electronic ballot boxes were used in all cities of more than 200'000 inhabitants and all states' capitals. Altogether, a third of the electorate had access to electronic voting (33 million voters). 1998 (national election): electronic ballot boxes were used in all cities of more than 40,000 inhabitants. Altogether, two thirds of the electorate had access to electronic voting (75 million voters). 2000 (municipal and regional election): 1st nationwide all electronic ballot. 2002 (national election). 400,000 electronic ballot boxes used, some 115 million voters. 2004 (municipal and regional election). 2005: national referendum on the prohibition of the commerce of personal firearms and ammunition. 2006 (national election). 2008 (municipal and regional election), 450,000 electronic ballot boxes used, some 120 million voters. 2010 (national election). Turnout is growing as illiterates have been voting more since the introduction of electronic ballot boxes.
Voter Identification Mechanisms	Voters show their electoral card (without photo). The polling staff check it against the list of voters registered in the precinct and types the voter's registration number in their control terminal to ensure they have not already cast a ballot. Then the voter types their voter ID number on the voting terminal's keyboard and makes sure that the name that comes up is correct. The machine displays a list of candidates with a picture. The voter types the number of the candidate of their choice and presses the green "confirm" button. Poll workers could vote for voters who do not show up, provided they are organized. As poll workers are randomly selected, this risk is considered minimal. To further reduce this risk, the nationwide deployment of a voting machine with a touchscreen allowing voters' fingerprint recognition is planned for 2018. A pilot program of the

	biometric identification technology was carried out in the 2010 presidential election, with the participation of over 1.2 million voters in 60 municipalities of 23 states.
Audit Trail	As a consequence of fraud in the senate electronic voting system in 2001, a law mandating a paper trail on the electronic ballot boxes was adopted. However, the testing of the paper trail in 2002 (in 5% of all precincts) was done in such a way that it failed, after which the law was revoked in 2003. In 2009, the parliament has reintroduced the obligation of a paper trail. It will be effective in 2014. The SEC will manually count 2% of all cast ballots for verification purposes.
E-Voting System Provider	The first Brazilian voting machine, known as UE96, has been developed in partnership by three companies: OMNITECH, Microbase and Unisys do Brasil. In 1998, Diebold-Procomp, Microbase and Samurai (formerly OMNITECH) partnered to produce UE98. In 2000, Microbase and Diebold-Procomp developed the UE2000. In 2002, Diebold-Procomp partnered with Microsoft. The new machines moved away from a DOS operating system to Windows CE. In 2004, Diebold-Procomp migrated to Linux.
Intellectual Property Rights of the E-Voting System	The supplier owns the intellectual property rights for the system. This is built according to specifications issued by the SEC.
Open/Closed Source Code	The source code is proprietary. Experts mandated by the SEC or the political parties have to sign a non-disclosure agreement that prevents them from publicly reporting their findings. The use of compilation tools is not allowed.
System Testing and Certification Mechanisms	One hundred eighty days before Election Day, the political parties and their IT experts, the Brazilian Bar Association, the Public Prosecutor Office and "any citizens with credentials with the Electoral Justice" are invited to analyze the electronic ballot box software, but not the source code, in an SEC-controlled environment. Then, they digitally sign the software together with the SEC. A piece of software developed by the SEC is then used to verify the proper compilation of the machines' software and the correctness of the hash produced. The fact that this is not performed by a piece of software developed by a third party has been criticized as being a mere self-certification by the machine. The Regional Electoral Courts issue the memory cards and diskettes containing the voters' list and the candidates' list for the precincts in their area. The parties invited to analyze the voting software can attend the production of the memory devices. Each vote is digitally signed and stored on two different flash cards. The tallying of each machine is digitally signed by the president of the precinct and sent to the Regional Electoral Court using a secure connection. The consolidating system only accepts one file per precinct.
Transparency Mechanisms	The SEC mandates universities to audit the system, but the audit reports are not public. On the eve of an election, the election authorities in each state select three percent of the machine by drawing of lots. The selected machines are kept in the premises Regional Electoral Court for a "parallel voting" conducted in the presence of representatives of the political parties and the media. This mock election takes place

	on Election Day. The whole audit is filmed. The outcome of this predictive test must match the expected results. At 7 am on Election Day, a "zero record" is produced for each electronic ballot box, in the presence of political parties' representatives, to prove that the machine's memory is empty.
Court Cases Against the Use of E-Voting	Legal cases are dealt with by the SEC, which is in the position of judge and jury. In 2000, in Santo Estevao (state of Bahia), an unelected candidate to the state parliament hired an expert to audit the electronic ballot box. The expert discovered that the machines were "self-certified" and sent the SEC a list of questions, which were never answered. In 2002, the Partido Democratico Trabalhista (PDT or Democratic Labour Party, which averages 4 to 5% of votes in national elections), the Partido Socialista Brasileiro (PSB, 4 to 7%) and the Partido do Movimiento Democratico Brasileiro (PMDB, 15 to 17%) appealed to the SEC against the way electronic voting had been run for the 2002 elections. The PDT challenged the software validation process involving the political parties, the Brazilian Bar Association and the Public Prosecutor Office because the software presented had already been compiled. The PSB challenged the absence of any identification on the voting machine's memory devices and the self-certifying property of the machine. The PMDB challenged the validation process, the use of unprotected memory devices in the voting machines and the procurement process. All complaints were rejected. No other court case was filed.
Key reports on the system	"Personal lessons from Brazil's pioneering experience with e-Vote", Pedro A.D. Rezende, 2007. "Digital Democratization: Suffrage Expansion and the Decline of Political Machines in Brazil", F. Daniel Hidalgo, UC Berkeley, 2010. "Concurso das Mais Estupidas Medidas de Segurança" organized by the NGO Privacy International (www.brunazo.eng.br/voto-e/PIcontest/)

Data Sheet – Non Remote E-Voting
France

Background	France began using e-voting machines in 2004. According to the explanations provided by the electoral authorities, organizational issues led to this decision because it would have been increasingly difficult to recruit enough people to administer elections, while e-voting seemed to ease those organizational needs. Each e-voting system needs to be authorized by the central French authorities, but the final decision belongs to each municipality on whether to continue with paper means or choose one of the systems previously certified by the Ministry. After the 2007 presidential and parliamentary elections, the government created a working group that assessed the experiences already carried out and suggested to continue using voting machines provided some adaptations were included both in legal, statutory and technical regulations.
Years of Use	2004 – 2011
Type of Elections/Referenda	2004 (regional / cantonal) 2004 (European Parliament) 2005 (European Constitution referendum), 2007 (presidential and parliamentary elections), 2008 (local / cantonal) 2009 (European Parliament), 2010 (regional) 2011 (cantonal). Voting machines may also be used for those Senate constituencies that have proportional election methods.
Type of E-Voting System	The three e-voting solutions currently authorized are DRE systems, although each one has its own particular features.
Brief Description of E-Voting System	The system is only available in municipalities with more than 3,500 inhabitants and included in a list adopted by the governmental delegate (*préfet*). Right now there are three systems certified by the government: ES&S, Indra and Nedap. After the exhibition of an ID credential, voters cast their ballots in an isolated environment via a computer. Indra's solution also includes a smart card that is given to the voter in order to operate with the voting machine. This system adds two supplementary devices that intend to verify whether the card is ready to be used and whether the ballot has been actually cast. This second device is a key element in order to correctly fulfill the electoral roll because, according to French law, each voter should sign it after casting his/her ballot and the device is the way to achieve this verification. ES&S and Nedap have other ways to check whether the voter has already cast his/her ballot. E&S procedure inserts the ballot activator cartridge for each new voting session and Nedap includes a wired connection, from the voting booth to the polling board, which provides this data.
Status of the E-Voting Option	Currently in use, but the list of municipalities may be different from one election to the next and there is no single reason for these decisions. It may depend on criticisms against voting machines, legal issues (e.g. the limitation to only one voting machine per polling station) or previous organizational failures (e.g. the queues generated during the first round of the 2007 presidential election).
Eligible Voters	Citizens eligible to vote are the same as in traditional voting means. There is no specific registration or identification procedures since both steps are prior to the use of voting machines. Where e-voting is implemented, it is the only voting channel.
Other Voting Channels Available	Proxy-voting
Period of E-Voting	Only during Election Day.

Legal Basis for E-Voting	The legal basis is the same since 1969 when France started using mechanic (not electronic) voting machines. In 2003, a detailed technical regulation ruled the procedure to certify e-voting machines and subsequently the government agreed on three voting platforms. The Constitutional Court also analyzes the electoral procedure and, beyond binding decisions, it also provides recommendations and an overall assessment.
E-Voting Usage	During the first round of the 2007 presidential election, 83 cities used voting machines. This makes up approximately 1.5 million voters or three percent of the electorate. NEDAP ESF1 was used in 68 cities, ES&S iVotronic in eight cities and INDRA "Point&Vote Plus" in seven cities. New cities have not been recently authorized to use electronic means and the actual number of cities involved decreased for subsequent elections.
Voter Identification Mechanisms	Voting machines do not change traditional identification procedures.
Audit Trail	Neither paper trail nor E2E verification are foreseen.
E-Voting System Provider	ES&S Datamatique / iVotronic voting machine Indra Sistemas / Point & Vote voting machine Nedap – France Elections / ESF1 (HW 1.06/2.01 - FW 4.02) voting machine (new model certified in 2007)
Intellectual Property Rights of the E-Voting System	Each private provider retains the full ownership of the e-voting system and only licenses the French government to use it.
Open/Closed Source Code	The source code is disclosed to the entities that conducted the previous certification and also to the Government.
System Testing and Certification Mechanisms	Each system is submitted to a previous certification that intends to verify whether it complies with the requirements included in the technical regulations. Once authorized by the government, the e-voting system and its implementation by the supplier should be followed up by a certifying body with a visit at least every two years. Major updates also need a new certification. The certifying body is selected and paid for by the supplier among those previously agreed by the Ministry.
Transparency Mechanisms	Key documents regarding the certification (e.g. report of the certifying entity, source code) are not published. The official body dealing with the access to public information rejected a demand on the basis that such data might endanger industrial property and the correct performance of the elections.
Court Cases Against the Use of E-Voting	The 2007 presidential and parliamentary elections generated several lawsuits that aimed to stop the implementation on the basis of some given features of the machines that did not seem to comply with the technical specifications set up by the Ministry. None of these lawsuits achieved its goal, but they led to a partial disclosure of the certification report gave to Nedap's machines. The Constitutional Council also had to solve some legal challenges, one of them addressing whether a polling station could include more than one voting machine. Some municipalities adopted this solution, but article L63 of the electoral code avoids it (CC 4 October 2007, *A.N., Marne, 3ème circ.).* Subsequent elections were conducted with less legal challenges.

Key Reports/Documents	Ministry of Interior / Section “Voting Machines” — http://ves.cat/aQc6 Constitutional Council / Section “Voting Machines” – http://ves.cat/aQaH Ordinaterus-de-Vote — www.ordinateurs-de-vote.org Observatoire du Vote — http://w3.observatoire-du-vote.eu

Data Sheet – Non Remote E-Voting
India

Introduction	In the 1970s, the electoral process in India was confronted with three main problems, made more challenging by the sheer size of the country: the logistics of elections, the empowerment of illiterate voters, and recurrent vote rigging. Vote rigging took the shape of ballot boxes disappearing and reappearing full of illegitimate ballots; voters turning up at the polling station to discover that they had already voted; trucks carrying sealed ballot boxes being hijacked on the way to the tallying center; and thugs invading the polling stations, stuffing the ballot boxes and chasing all voters away. In every election since the country's independence in 1947, the number of invalid votes (linked to illiteracy) was more than the winning margin between candidates. Electronic voting machines put an end to these problems. In 2007, the literacy rate was 66%. In 1977, the Electoral Commission of India (ECI), a constitutionally created body, started studying mechanized voting. An official committee issued a recommendation in favor of direct recording electronic systems. It was deemed necessary to develop a voting machine that would be suitable for illiterate voters. The machine needed to be simple enough to inspire trust. The Electronic Voting Machines (EVM) were first used in 1982 in the Parur Assembly Constituency of Kerala in 50 polling stations. The first generation EVMs (1980-2000) were functionally similar to the current ones. The main difference is that the firmware was stored on a diskette instead of being burnt into the CPU. The deployment of EVMs progressed slowly, as their use and impact was being tested. The first nationwide deployment of the EVM took place in 1999.
Years of Use	1999: general election, in some states only. 2004 (1st nationwide eEnabled ballot): general election. 417 million votes cast 2009: general election Over 30 elections for state assemblies between 2004 and 2009.
Type of Elections/Referenda	Regional and general elections.
Type of E-Voting System	Stand alone direct recording machines.
Brief Description of E-Voting System	The EVM is made of two devices running on six volt batteries. One device is the voting unit, the other is the control unit operated by the electoral officer. They are connected by a five meter cable. The voting unit has one button per candidate (16 buttons on the unit, although it is possible to link up to four units to accommodate 64 candidates). The candidates' name and party symbols are displayed next to the corresponding button so that illiterate citizens can vote. The control unit has three buttons: one to release a single vote, one to check the total number of votes cast at any point in time, and one to close the voting process. The result button is hidden and sealed and cannot be pressed unless the close button has been pressed. Machines can only record five votes per minute to avoid ballot stuffing by thugs invading the polling station. For the same reason, a maximum of 3,840 votes can be

	recorded in a single EVM. EVM are plain circuits with some assembly code. The software is embedded in the hardware so that it cannot be reprogrammed. In 2006, after a report by an Expert Committee set up by the ECI, some features were added: dynamic coding between the ballot unit and control unit, installation of real time clock in the machines, installation of a full display system and date and time stamping of every key pressing n the machine. The machines fitted with these features were called “new” machines, by comparison to the “old” ones which were unchanged. After the vote, the EVMs are brought to counting centers, where the outcome of the election is tallied. 1.378 million EVMs were used in the 2009 general election, 930,000 old ones and 448,000 new ones.
Status of the E-Voting Option	Currently being used.
Eligible Voters	Seven hundred and fourteen million Indian citizens over the age of 18 (data from the 2009 general election).
Other Voting Channels Available	None
Period of E-Voting	The election process in India takes at least a month for state assembly elections, with the duration increasing further for general elections. The 2009 general election took place in five phases, between 16 April 2009 and 13 May 2009. No vote is counted until the last state has finished voting. The results are then published in one day.
Legal Basis for E-Voting	Indian electoral law.
E-Voting Usage	The entire electorate.
Voter Identification Mechanisms	Voters must present their voter identity card or their public distribution system’s ration card. Their name is then found in the electoral register. After they have cast their ballot, voters’ fingers are marked with an indelible ink that lasts two weeks, to prevent them from voting again.
Audit Trail	Upon court order, it is possible to print out the content of an EVM’s memory. A Kerela court requested this in 2002. In July 2011, an EVM with paper trail was tested in 200 polling stations.
E-Voting System Provider	Indian EVM are designed and produced by two government owned manufacturing units, Bharat Electronics Limited (BEL, belongs to the Ministry of defense) and Electronics Corporation of India (ECIL, belongs to the Department of atomic energy). Both systems are identical and are developed to the specifications of the ECI. These two companies are not under the administrative control of the ECI.
Intellectual Property Rights of the E-Voting System	The Indian federal state.
Open/Closed Source Code	Closed. The code is burnt into the CPU by a Japanese company called Renesas and an American company called Microchip. The ECI has no access to the source code after it is burnt into the microprocessor.
System Testing and	The certification (compliance with functional requirements) is done by the EVMs’

Certification Mechanisms	suppliers, on prototypes. Samples of EVMs from production batches are also regularly checked for functionality. The software is tested against the specifications by an “independent testing group”, as the ECI states. After this test, the code is given to the machines manufacturer to be fused into the CPU. Only “black box“ testing is possible (functionality tests) as the ECI does not let anyone access the code and the industrial process of burning it into the microprocessor Before any ballot is cast, each EVM is inspected by a technician. Preparation of EVMs for elections and their sealing is done in the presence of candidates or their representatives. They sign the thread seals applied on the machines after the preparation. EVMs are then kept in strong rooms until the election. Candidates can place seals on the doors of the strong room. Since 2006, a mock poll is always conducted on 10 percent of the machines to ensure the proper recording of votes. A certificate is issued for each machine after this mock poll.
Transparency Mechanisms	There is a two-level randomization (constituencies and polling stations) process in the allocation of EVM to precincts in the country to avoid any preprogramming of the machines. This randomization takes place with the involvement of candidates or their representative.
Court Cases Against the Use of E-Voting	As in any case of electronic voting implementation, the introduction of electronic voting in India provoked its share of criticism. But the debate around the use of EVM and the legal complaints and political infighting increased after the 2009 general election, which saw the surprise victory of the outgoing government coalition led by the Congress Party. In 2001, the Madras High Court rejected the idea that the machines could be tampered with. The Karnataka High Court, in a similar case that it dismissed, wrote that the EVMs were a national pride. Following the 2009 general election, Shri V.V. Rao and three other members of the Jan Chaitankya Vedka (a NGO) brought a case to the Supreme Court raising questions about the EVMs, but not producing evidence. The court said they could directly address the ECI. Similar petitions were raised by the Bombay High Court, the Madras High Court, the Orissa High Court and the Madhya Pradesh High Court, claiming that it was possible to tamper with the EVM either during the manufacturing process, or during the operation of the machines. The Supreme Court dismissed these claims. In August 2009, the ECI invited “those who (had) recently expressed reservations about the EVM, to come and demonstrate the points made in their allegations” on the ECI premises. Doubters were given from August 3 to August 8 to approach 100 EVMs for scrutiny. As the ECI writes, “None of the persons who were given the opportunity could actually demonstrate any tamperability of the ECI-EVM.” They either failed or chose not to demonstrate. The ECI has however not succeeded in calming fears. In June 2010, 13 political parties submitted a joint memorandum to the ECI demanding a review of the EVM use. This was prompted by the demonstration made in April 2010, by Hari Prasad, Rop Gonggrijp, J. Alex Halderman et al. of two attacks that they carried out on an EVM, as well as descriptions of several other potentential vulnerabilities. One attack was based on replacing the part inside the control unit that actually

	displays the candidates' vote totals. The study showed how a substitute, "dishonest" part could output fraudulent election results. The second demonstration attack used a small clip-on device to manipulate the vote storage memory inside the machine. The ECI claimed that the EVM used for the testing was a fake one and pointed out that, in any case of tampering with the EVMs, one needs both physical access to them and high technical skills. In addition, to affect the results of an election, hundreds to thousands of machines would be needed. Some have also noted that all political parties criticizing the EVMs have lost the recent elections.
Key reports on the system	Election Commission of India Website - http://eci.nic.in/eci_main/faq/evm.asp Election Commission of India Press Note of August 8, 2009 - http://eci.nic.in/eci_main/press/current/pn080809.pdf "Security Analysis of India's Electronic Voting Machines", Hari K. Prasad, J. Alex Halderman, Rop Gonggrip et al., April 2010 at http://indiaevm.org/ "Democracy at risk", GVL Narasimha Rao, published by Veta (Citizens for Verifiability, Transparency and Accountability in Elections), New Delhi, 2010.

Data Sheet – Non Remote E-Voting
The Netherlands

Background	In 1965, a legal provision was passed allowing the use of machines for voting and counting. In 1966, the first attempts were made to automate the counting process. The next year, the government passed the first rules for the approval of voting machines, but it took until 1997 to pass technical regulations on electronic voting machine standards. Since 1994, the use of electronic voting machines has continued to increase. In 2006, 97.7% of Dutch municipalities used electronic voting machines. Criticisms of the use of electronic voting machines started from 2000, with the main concerns related to the secrecy of the source code and evaluation reports, and the lack of verifiability of the machines. However, it took developments in Ireland, which were using the same NEDAP machines as the Netherlands and the introduction of voting machines to the city of Amsterdam, to bring these concerns to fruition. Ireland used NEDAP machines in a 2002 pilot for electronic voting. It intended to implement the machines nationwide, but in the face of public opposition established an Independent Commission on Electronic Voting and Counting at Elections to review the suitability of the machines it procured. The Commission, which published reports in 2004 and 2006, identified concerns which, while they could be addressed, did not make the machines fit for use in Irish elections. These main issues were concerns about the accuracy of the system due to insufficient testing and the fact that changes were still being made to the system, not providing sufficient time to retest the system before its planned use. Concerns were also raised about possible violations of vote secrecy resulting from preference votes under the SNTV system and the lack of a voter-verified audit trail. These findings led Dutch citizens to start asking similar questions which culminated in the establishment of a pressure group called "We don't trust voting computers" in late 2006. The pressure group managed to buy some NEDAP machines and identified a number of security flaws in the machines, including the easy replacement of program chips allowing the results to be manipulated. Due to the lack of verification mechanisms, such replacements would go unnoticed. The susceptibility to eavesdropping on the radio emissions of the voting machines was also demonstrated. In 2006, the government established two committees to look into the issue of electronic voting. In April, the Voting Machines Decisions Committee issued a report entitled 'Voting Machines, a neglected dossier'. This report listed recommendations for both the short and medium terms about voting machines legislation. Autumn saw the publication of the report 'Voting with confidence' issued by the Advisory Committee on the Voting Process Mechanism, after which the cabinet adopted a position on the matter. The Election Process Advisory Committee's report, published in September 2007, recommended that due to issues of transparency and verifiability voting should take place using only paper ballots in polling stations and effectively ended the Netherlands' use of electronic voting machines. While the Committee's report did not rule out the possibility of electronic voting machines in the future, which better met the requirements of elections in the Netherlands, there have been no moves to introduce new electronic voting machines. In October 2007, the regulation allowing the use of electronic voting machines was withdrawn.
Years of Use	Early 1990's – 2006

Type of Elections/Referenda	European, Parliamentary and Local Government
Type of E-Voting System	The most recent electronic voting machines used in the Netherlands were direct recording electronic voting machines, some with buttons for each of the candidates running for election (NEDAP) with others using touch screens (SDU).
Brief Description of E-Voting System	In order to vote using the NEDAP machine, by far the most widespread machine that was used in the Netherlands, a voter touches the spot on the machine which is labeled for their candidate of choice. The machine is touch sensitive and covered by a ballot paper which identifies all of the candidates. The voter's choice is displayed on a small screen on the voting machine and the voter must confirm this choice by pressing a red button, which commits the vote to the electronic ballot box. At the end of the session, the machine prints out the results on the machine.
Status of the E-Voting Option	Discontinued
Eligible Voters	Decisions on the implementation of electronic voting machines were made at the local level. In 2006, the last election to use electronic voting machines, 97.7% of Dutch municipalities used electronic voting machines. The machines were the only voting channel available in the polling stations that used them.
Other Voting Channels Available	In polling stations using electronic voting, no paper ballot options were available. Proxy voting has also been available for voters since 1928, and this is meant to be used in case of illness or absence. This does not need to be pre-approved, but is merely done by the voter signing the voter card and the proxy using this to vote on Election Day. A proxy can only cast two proxy votes in an election. Postal voting is available since 1983 for voters living abroad or with work duties abroad on Election Day. Postal voting is not available for voters in the Netherlands. The Dutch government has also experimented with remote e-voting, with voters from abroad able to vote through the Internet in the 2004 and 2006 elections. In 2008 the government decided to cease all e-voting methods, including the Internet voting experiment
Period of E-Voting	Election Day in polling stations
Legal Basis for E-Voting	The Elections Act - http://www.lexadin.nl/wlg/legis/nofr/eur/lxwened.htm
E-Voting Usage	Usage of voting machines grew over time, but by the 2006 election 97.7% of municipalities in the Netherlands were using electronic voting machines to vote.
Voter Identification Mechanisms	Since 2009, voters have to show an official identification document before they can vote. Prior to this, it was sufficient to hand over the polling card that eligible voters received two weeks before Election Day.
Audit Trail	No audit trail existed in any of the voting machines used
E-Voting System Provider	NEDAP and SDU
Intellectual Property Rights of the E-Voting System	The suppliers owned the intellectual property rights

Open/Closed Source Code	Access to the source code was provided after the election.
System Testing and Certification Mechanisms	The minister would approve the machines, based on a report by TNO. In 1997, a regulation on voting machines was established, including an extensive list of requirements that voting machines had to meet. Demands on the verifiability of the counting, however, largely remained unspecified. Voting machines in the Netherlands had to be approved by an evaluation institute. Although multiple institutes could be designated in principle, only TNO has been involved in this procedure thus far. Only TNO (the department doing the evaluation now being called BrightSight) was given the source code of the software running on the machines.
Transparency Mechanisms	System documents were made available.
Court Cases Against the Use of E-Voting	In 2007-2008, there have been a few court cases involving the withdrawal of the voting machine: www.rechtspraak.nl: LJN: BB4541, Rechtbank Amsterdam, AWB 07/2340 en AWB 07/2268 LJN: BA7269, Rechtbank Amsterdam , 368844 / KG ZA 07-801 AB/MB
Key Reports/Documents	OSCE (2006) – The Netherlands Parliamentary Elections 22 November 2006: OSCE/ODIHR Election Assessment Mission Report Gonggrijp, R. and Hengeveld, W-J.(2007) – Studying the NEDAP/Groenendaal Voting Computer: a security perspective, paper presented at USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, USA Election Process Advisory Commission (2007) – Voting With Confidence - http://www.kiesraad.nl/nl/Overige_Content/Bestanden/Engelse_website/Voting_with_confidence.pdf

Data Sheet – Non Remote E-Voting
United States-State of Maryland

Background	Maryland, like many U.S. states, decided to review its voting system after the disputed 2000 presidential election. In that election, contested results from the state of Florida highlighted significant problems with election administration in the country. In 2001, Maryland Governor Parris Glendening established a special committee to review the state's election operations. The committee recommended statewide electronic voting. In 2001, Governor Glendening signed House Bill 1457, which required a uniform system to be used across all counties in the state. On September 12, 2006 the state introduced the introduced electronic poll books (EPBs), which are described in more detail below.
Years of Use	2002 – 2011 (present)
Type of Elections/Referenda	2006 Primary and General elections. 2008 Primary and General elections. 2010 Primary and General elections.
Type of E-Voting System	AccuVote-TS, a touchscreen voting system by Election Systems and Software Inc. The model was initially produced by Premier Election Solutions (more commonly known by their old name, Diebold), but Election Systems and Software acquired Premier Election Solutions in September 2009.
Brief Description of E-Voting System	The system is available throughout Maryland and the number of units per polling station is determined by the amount of constituents in the district. When a voter enters the station, they are registered in the electronic poll book (EPB). EPBs find a voter (countywide or statewide) and if in the correct polling place, a voter access card is inserted in the EPB, which encodes it to allow voting. In addition, when connected to a printer it prints the voter authority card (VAC). If they are in the system, they are given a one-time use Voter Access Card (VAC). This card is then inserted into the voting machine and the ballot appears on the touch screen. Once the ballot is cast, the VAC is erased and ejected from the voting unit. The VAC is then returned and is available for use with another voter. Before polling stations are opened, all machines are verified to be "Zeroed" out meaning there are no votes currently in the unit. Throughout the day, counts are taken on the machine to verify the number of votes cast equals the number of voter access cards issued. Headsets and keypads are attached to one unit to facilitate disabled citizens. After polls have closed, a poll worker inserts an administrator card into each voting machine and puts the machine into a post-election mode where it will no longer record votes. The machine then copies the data onto the card, which is taken to a central tabulation facility.
Status of the E-Voting Option	E-voting is currently being used throughout Maryland for early voting and voting on election day. Provisional ballots are offered on paper for non-registered voters and voters that appear at the wrong polling station. Mail-in absentee ballots are available upon request.
Eligible Voters	Citizens entitled to vote are the same as in traditional voting means. Registration is preferred but voters can still vote using a paper provisional ballot if they are not registered in the voter poll book. No identification is necessary to vote. ID is checked against the voter electronic poll book.
Other Voting Channels Available	Absentee mail-in ballots are available. For both absentee voting and provisional ballots, voters use a paper-based optical scan voting system (AccuVote-OS or Model

	ES-2000). Early voting is also available, using the standard DRE.
Period of E-Voting	On Election Day, both for general elections and primaries. Also, to accommodate early voting, four to five days prior to the election at a reduced number of locations around the state. The number of early voting polling stations per county is determined by number of registered voters in each county.
Legal Basis for E-Voting	Maryland General Assembly, House Bill 1457 (2001), which required the State Board of Elections, in consultation with the local boards of elections, to select and certify a voting system for voting, as well as requiring the selected and certified system be used in all counties. In addition, electronic voting machines ensure that Maryland is compliant with the Help America Vote Act (HAVA) of 2002, which requires that every polling station be accessible to voters with disabilities.
E-Voting Usage	The touch screen DRE machines are used throughout the state. Paper provisional ballots are provided to voters if there is a question regarding the voter's identity or correct polling station.
Voter Identification Mechanisms	No proof of identification is necessary to vote. Voters' identity is checked against the voter electronic poll book.
Audit Trail	At the moment, there is no paper trail for the voter. In 2005, the Maryland General Assembly passed Senate Bill 849 and House Bill 479, which required the State Administrator of Elections to conduct a study of independent verification systems. Governor Robert L. Ehrlich, Jr., however, vetoed the legislation. In 2007, Governor Martin O'Malley signed into law, SB 392, which called for replacing Maryland's paperless touch-screen voting system with a system that produces a paper record. The transition, however, was delayed after the State Board of Elections (SBOE) estimated that the cost of the switch would be too high. Each voting unit does print a report before the polls open confirming that there are no votes on the voting unit. After the polls close, another report is printed showing the results from that voting unit. Additionally, in case of a recount, ballot images can be printed from the election database. These ballot images can be manually recounted without being attributable to any particular voter.
E-Voting System Provider	Election Systems and Software Inc.
Intellectual Property Rights of the E-Voting System	Election Systems and Software Inc.
Open/Closed Source Code	The source code is closed. However, much debate has been made about a leak of the code on the Internet that was shown to be vulnerable to fraud by a professor at Johns Hopkins University. There has been debate as to the authenticity of the leaked code with the vendor saying it was not the latest version and several generations old.
System Testing and Certification Mechanisms	Maryland law requires that a voting system be examined by a federally appointed independent testing authority (ITA) and be shown by the ITA to meet the federal performance and test standards for electronic voting systems. An ITA conducts a comprehensive testing process on the hardware and software of the voting system and performs a review of the source code. Second, a voting system must be certified for use in Maryland. Certification involves

	end-to-end testing of the voting system. Third, after the ballots are loaded on each voting unit, a pre-election test is performed on each voting unit. During this test, elections officials confirm that the results match the expected outcome. After confirmation, the voting units are cleared of all votes and sealed and secured until Election Day. Lastly, Maryland has implemented a thorough public testing demonstration and parallel testing program. This program will involve randomly selecting voting units and voting scripted ballots to confirm the accuracy of the voting system.
Transparency Mechanisms	Prior to an election, voting units are stored in a locked warehouse, in which only authorized individuals can enter. Election officials must pass a criminal background check to gain access to the election database. The voting units are sealed until Election Day morning when they are opened by sworn, bipartisan election judges. Election judges confirm that there is tamper tape covering access to the compartment with the power button and memory card. During Election Day, election judges ensure that only registered voters use the voting equipment and continuously monitor voting. Throughout the day, election judges compare the number of voters recorded as voting against the number of votes cast on the voting units and would identify any discrepancies immediately. After the polls close, election judges compare the vote totals generated by the voting units against the voter turnout totals recorded by the election judges. A sworn, bi-partisan team of election judges transports the memory cards to the election office. During transit, the voting units are again sealed, and access to the memory cards is restricted to specific election officials.
Court Cases Against the Use of E-Voting	In 2004, a group of Maryland voters filed a lawsuit against the Maryland State Board of Elections arguing that the Maryland DRE machines failed to comply with both state and federal law. A judge ruled in favor of the state in 2004, but the case was appealed several weeks later. The state Appeals Court upheld the ruling in 2007.
Reports/Documents	*Science Applications International Corporation (SAIC)* • Risk Assessment Report - Premier AccuVote-TS Voting System and Processes • SBE's Response to Risk Assessment Report: Voting System Action Plan (updated July 7, 2004) • SBE's Letter Accompanying the Voting System Action Plan *Department of Legislative Services (DLS)* • Review of Issues Relating to the Premier AccuVote-TS Voting System by the Dept. of Legislative Services • Trusted Agent Report – Premier AccuVote-TS Voting System by RABA Technologies • SBE's Response to DLS' Trusted Agent Report on Premier AccuVote-TS Voting System (updated July 22, 2004) *Freeman, Craft, McGregor Group Report* • Report from a Review of Maryland's Voting Sytem by the Freeman, Craft, McGregor Group

	National Center for the Study of Elections of the Maryland Institute for Policy Analysis & Research University of Maryland, Baltimore County • Maryland Registered Voters’ Opinions About Voting and Voting Technologies by National Center for the Study of Elections of the Maryland Institute for Policy Analysis & Research University of Maryland, Baltimore County