Online voting: a legal perspective[1]

Mieke Loncke and Jos Dumortier

K.U.Leuven – ICRI
Tiensestraat 41
B-3000 Leuven – Belgium
icri@law.kuleuven.ac.be
http://www.law.kuleuven.ac.be/icri

Abstract. Casting a vote for the European Parliament from a cybercafe in Chile, a cruise ship in the Atlantic Ocean, a weekend cottage in the Alps or plainly at home from your laptop computer? This article tackles this question from a legal point of view. It examines the basic principles surrounding online voting. Are the conditions for democratic elections – such as the freedom to vote without undue influence or coercion of any kind, the secrecy of the vote, the integrity, reliability and security of the ballot box, the verifiability and audit ability of the voting process and the principle of one person, one vote – sufficiently met or do we run into legal obstacles? Does the introduction of an electronic or even online voting process jeopardize the principles of non-discriminatory access to the election process? And what about the anonymity? How can one guarantee that a vote over the Internet is cast by the legitimate voter, all the while guaranteeing his privacy? The last chapter of the article briefly touches the current state of affairs within the European Union. Is the introduction of online voting merely a science fictional feature or really within reach?

Introduction

Online voting easily captures people's interest as being a modern and contemporary alternative for traditional elections: the vote can easily be cast and efficiently processed, the results are rapidly available, archiving is less troublesome, etc. Online voting is also an appealing alternative for citizens residing abroad and for voters who are ill or disabled.

Despite the many obvious benefits of implementing online voting, the topic is riddled with pitfalls that must be carefully dealt with for such an election system to be

[1] Acknowledgments: This contribution is based on ICRI's legal research in the CyberVote project. [http://www.eucybervote.org]. The legal research in this project has been performed by Mieke Loncke, Frederic Debusseré and Bart Van Oudenhove, under the supervision of Jos Dumortier.

J. Padget, R. Neira, J. Díaz de León (Eds.). e-Government and e-Democracy: Progress and Challenges

successful. In particular, issues of voting privacy, security and integrity belong to the core of the voting process and must be addressed in any electoral system.

Online voting is doing a fine job trying to throw off its negative image, all the while being gratefully supported by more or less successful (pilot) projects all over Europe. In anticipation of the elections within the European Parliament of the European Union, scheduled for June 2004, the issue acquires more and more the attention of the public. But still, some convincing arguments could persuade critics to take another look at online voting.

1. What is an Online Voting System?

1.1. The Notion of an Online Voting System

Elections may be organised in many different ways. Paper based elections make use of paper ballots, while automated elections make use of some kind of voting machines, which automate the voting and/or tabulation procedures. When computers are used as voting machines, we talk about electronic voting.

Electronic voting systems may be further divided into off-line and online voting systems.

In an *off-line* voting system the computer is to be seen as a stand-alone computer, whereas in an *online* voting system, the computers are connected in a (closed or open) network. If the Internet functions as network, the term 'Internet voting' is sometimes being used.

As for Internet voting, two main types can be distinguished: polling place Internet voting and remote Internet voting [1].

A *polling place Internet voting system* uses Internet voting computers at traditional polling places, staffed by election officials who assist in the authentication of voters before the ballots are cast. This system doesn't require a digital authentication for the authentication can be done physically, similar to traditional or electronic elections. When the voter is authenticated, he can cast his vote anonymously. A *remote Internet voting system* uses unsupervised Internet voting computers to cast a ballot over the Internet, using a computer not necessarily owned and operated by the election personnel. This system requires electronic (for instance digital) authentication: the voter will need a personal key (password, digital signature) to identify himself as legitimate voter. Authentication is indispensable to guarantee the one man, one vote principle. However, the link between the authenticated voter and the cast ballot must be cut, so as to disable any tracing back.

Undoubtedly an Internet voting system should be introduced gradually. In this respect, an implementation in four stages is highly recommended: (1) Internet voting at voters' polling place, (2) Internet voting at any polling place, (3) remote Internet

voting from county-controlled computers or kiosks and in a last phase (4) remote Internet voting from any Internet-connected computer.

1.2. Internet Voting Compared to Absentee Voting

Postal voting is the most widespread form of *early or absentee voting*. In many ways Internet votes can be thought of as the electronic equivalent of paper absentee ballots. Both allow ballots to be cast remotely, basically from anywhere in the world, and at any time convenient to the voter within a certain time span before the actual election day. While the two methods inevitably give rise to similar concerns about lost ballots or call for similar mechanisms in order to prevent or detect double voting and to guarantee ballot secrecy, there are still some significant differences. For instance, e-voting systems can immediately provide the voter with feedback concerning the reception and acceptance of his ballot, whereas in case of absentee ballots sent through the mail there is no automatic indication to the voter that the vote has arrived, or arrived on time. The most important difference however is that e-voting raises security issues that have no analogue in the absentee ballot system.

2. Basic Principles

The question whether online voting could conform to the basic election rights, as laid down in international and regional convents and in national constitutions, will need to be explored further.

Allowing people to cast their vote online, via electronic communications networks, could jeopardize the following basic requirements, characteristic of genuine elections.

2.1. Equal, Non-discriminatory Access to the Election Process

The principle of non-discrimination and equality is a basic right in a democratic society. It ensures the right of every citizen to enjoy his rights and freedoms without discrimination. According to this constitutional requirement, every eligible voter can participate in the election process and nobody can – directly or indirectly – be excluded or discriminated.

2.1.1. Regulation

The rights of non-discrimination and equality are generally and internationally recognised. Since these rights are embedded in international convents, they enjoy absolute priority over national law.[2]

[2] Article 2.1. of the International Convent on Civil and Political Rights states: "*Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant, without distinction of any kind, such as*

2.1.2. Generally. The principle of equality and non-discrimination prescribes that equal situations should be treated equally and unequal situations should be treated unequally, if such an approach would turn out to be necessary to enable everyone to enjoy their rights and freedoms without discrimination.

Nevertheless, this does not exclude certain categories of people to be treated distinctly, on the condition however that the criterion for the distinction is *objective* and *reasonable*. This has to be evaluated bearing in mind the goal and consequences of the proposed treatment. In short, the principle of equality is violated, if the distinct treatment is not reasonably proportional to the aimed goal.

The principle prohibits the government to unreasonably limit the rights and freedoms of one category of persons in comparison to the rights and freedoms of other categories. At the same time it carries with it the obligation to take positive action in order to ensure equality.

As far as elections are concerned, the government has to make sure that everyone is equally given the opportunity to participate in public elections. Consequently, the government not only has to avoid enacting laws which unreasonably discriminate certain categories of persons, but also has to ensure *equal accessibility* to the voting process. Government thus has to take active measures to enable absent, ill and disabled people to vote.

Equal access basically requires an easy access to the ballot box for all eligible voters, without discrimination against disabled persons, elderly, computer illiterates, etc. Existing voting systems tend to be poor at accommodating the needs of disabled voters. For example, blind voters have to trust election officials to read the ballots and enter their votes. Electronic voting systems on the other hand, are capable of supporting a diversity of interfaces to the voter [2]. However, the use of an online voting system may not result in complicating the access to the elections for a (large) part of the population. User-friendliness in its largest sense is a precondition for any (online) election system.

As regards the principle of equal accessibility, a distinction has to be made between the different types of online voting systems, namely (1) voting at a supervised poll site using electronic equipment, (2) voting at an unsupervised electronic kiosk and (3) remote online voting using the voter's equipment.

When online voting is allowed at the existing official *poll sites*, there will occur no difference in accessibility compared to traditional voting for these poll sites are equally accessible to all citizens. However, equality could be at risk, if some citizens

---

race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

Article 2 of the Universal Declaration of Human Rights states: "*Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.*"

are compelled to use the online voting system, while others can resort to traditional voting. If the online system proves not to comply with the standards for democratic elections in the same way as traditional voting systems (e.g. the online voting system doesn't offer the same security guarantees), there could indeed be an unreasonable discrimination between those who have access to a system that complies with the requirements for democratic elections and those who don't have access to such a system.

The implementation of a *remote online voting system* entails even more risks. In this scenario, votes aren't cast at traditional poll sites, but at any random location. Undoubtedly it would be discriminative if voting in public elections were allowed *only* from a PC at home or at work, and not at public places (official poll sites and 'kiosks'). This would unreasonably eliminate a large number of people who do not have access to a computer (or mobile phone[3]).

When a system of remote online voting *co-exists* with a poll site or kiosk online voting system, it becomes tricky to evaluate the equal accessibility. Though all voters are equal, they are treated distinctly: people who have Internet access (at home or in the workplace), are allowed to vote using those facilities; people who do not have the advantage of such access, are compelled to vote at a kiosk or poll site. In order to enhance equal access, election authorities should make every effort to grant all citizens, without distinction, easy access to the public terminals. Extending the voting period from only one day to more, consecutive days and the placement of voting machines all over the constituencies (in libraries, supermarkets, groceries, post offices, banks, etc.) could serve this purpose.

2.2. The Principle of Democratic Elections

With respect to (anonymous) online voting, the principle of democratic elections can't be ignored. Numerous international and national legislations prescribe the right to democratic elections.[4]

---

[3] Techniques have been developed to enable voting from a (specially adapted) mobile phone. E.g. the CyberVote project, for more information consult the official website at http://www.eucybervote.org.

[4] Article 25 of the International Covenant on Civil and Political Rights prescribes the following: "*Every citizen shall have the right and the opportunity, without any of the distinctions (...) and without unreasonable restrictions:(...) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors; (...)*"
Article 21 of the Universal Declaration of Human Rights states the following: "*(1) (2) (...) (3) The will of the people shall be the basis of the authority of government; this shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.*"
Article 3 of this Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms deals with the right to free elections: "*The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature.*"

2.2.1. The Freedom to Vote, without Undue Influence or Coercion of any Kind / Secrecy of the Vote. In order for elections to be free and fair, the elector has to be able to cast his vote without influence or coercion of any kind for this may distort or inhibit the free expression of his will. Voters should be granted the opportunity to form their opinion independently, without pressure of any kind, free from coercion, inducement or manipulative interference, without violence or even the threat of violence.

Secrecy and freedom are strictly related principles for secrecy is the precondition of the voter's free political decision. In democratic elections the link between the vote and the voter must be irreversible, so as to ensure the free casting of the votes [3]. Secrecy could be seen as a 'conditio sine qua non' for the non-coercibility of the vote. Only when the voting takes place in secret and the ballot remains secret during the voting process, one can guarantee that the voter is not coerced into casting a particular vote. In traditional voting procedures, the secrecy is 'physically' protected, whereas e-voting may make the virtual voting process extremely vulnerable to violations of this principle.

A. Secrecy. Anonymity and secrecy should be observed during the whole election process: (1) during the casting of the vote, (2) during the transfer of the vote from the client to the server and (3) after the transfer of the vote by the server.

(1) During the Casting of the Vote

In order to prevent the voter from being unduly influenced when casting his vote, absolute anonymity is required. This requirement however, can only be fully guaranteed in controlled physical circumstances in which the vote is cast. In traditional elections, voters are obliged to cast their vote in private voting booths at official poll sites. Similar material circumstances can only be established in a poll site or a kiosk online voting system for these conditions cannot be implemented and enforced in a remote online voting system. Currently it remains technically impossible to control the circumstances in which the remote votes are cast. Obviously, this can lead to abusive practices: the buying and selling of votes, coercion by family members or by employers or colleagues, etc. This raises serious concerns about the compliance of such an election system with the freedom to vote.

Concerns also relate to the problem of the authentication of the voter. A watertight, one hundred percent secure electronic authentication from a distance is not yet feasible. At the moment, existing technology is unable to guarantee that the voter, authenticated by the system, and the voter who is actually casting the vote, are one and the same.

Regarding these objections, some proponents of a remote online voting system point to exceptions provided for in existing election systems, to press home arguments. They refer to a number of traditional electoral systems which allows voters, ill, disabled or residing abroad, to cast an absentee ballot through ordinary mail. In that case, the non-coercibility has been compromised, in order to serve a higher purpose,

being the right to vote. However, it is to be seen as an exceptional procedure – applicable only to voters who are ill, disabled or residing abroad – created to enable specific categories of people to equally exercise their right to vote. As it is an exception, which serves a legitimate purpose, it can in principle not be generalised in order to become the general rule. On the other hand, it shows that there would be no legal impediment to introduce a remote online voting system for absent, ill or disabled persons. The system would only have to be at least as safe as the existing vote by mail systems.

Another argument in favour of a remote online voting system is that the freedom to vote is experienced less absolute in today's society. Although people nowadays have less scruples about their political preferences, the requirement of the freedom to vote is mainly kept alive to avoid anomalies (illegitimate influence), which will always exist. On the other hand however, an automated voting system would facilitate fraud on a larger scale than is possible today.

Finally, one cannot overlook the role of the Internet with regard to political advertisement and propaganda. The Internet is an ideal medium to enable people to cast an 'informed vote'. After all, the Internet offers enormous possibilities to diffuse the opinion of candidates and their parties and therefore becomes a major source of information on which electors can found their preference. This way the Internet can enhance the 'quality' of the vote and consequently the quality of democracy. Nevertheless, the situation is different when political advertisements pop up on the voting site without prior demand of the voter – like is often the case with commercial messages. Traditional election systems prohibit advertising in the polling place itself. Any Internet voting system should therefore make it technically impossible for such advertisements to appear on the voting website.

(2) During the Transfer of the Vote

During the voting procedure – that is, from the moment the encrypted ballot goes online to be transferred – no one, not even the official staff, may be able to link a particular vote with a particular content to a particular voter. This requirement is closely related to the security issue and can therefore be addressed on a technical level in particular by using advanced encryption methods: the system should implement secure technical measures, which would make it impossible for the secrecy of the vote to be breached. In a remote online voting system (possibly also in the kiosk voting system), these technical challenges are most daunting, since the system should not only authenticate eligible voters distantly, but it should also cut the connection between the voter and the ballot.

(3) After the Transfer of the Vote

The content of the ballots cast has to remain secret until the moment of tabulation. Therefore, as soon as the cast vote has been received by the system, it must be made technically impossible to find out the content of the vote. If this were possible, the non-coercibility would be jeopardized for votes could be bought, sold or coerced.

Once the vote has been cast, encrypted, sent and received by the system, it would be the safest never to reveal the content of the vote, not even to the voter himself. One could however consider enabling the system to send a confirmation of the receipt of the vote, including the content of the vote. However, this confirmation may never be communicated on a durable medium, like a printed receipt, or in a digital form, which could be saved on a carrier of any kind. This solution doesn't violate the secrecy requirements but allows the voter to correct mistakes before sending his final vote. In addition to increasing the voters' confidence, it also enhances the verifiability and reliability of the system.

Taking into account the foregoing, following requirements could be distilled from the principle of secrecy [4]:

- The secrecy of the vote has to be guaranteed during the casting, transfer, reception, collection and tabulation of the votes;
- None of the actors involved in the voting process (organizers, election officials, trusted third parties, voters, ...) should be able to link a vote to an identifiable voter;
- There must be a clear and evident separation between the registration and authentication procedures on the one hand and the casting and transfer of the vote on the other hand;
- No voter should be able to prove the content of his vote. The confirmation of the vote, after the transfer of the ballot, enforces the confidence in the system while ensuring the rights of the voter, but may under no circumstances relate to the content of the vote.

B. Freedom and Non-coercibility. Undue influence of the voter should be prevented. Cryptography can serve this purpose, however, it can only guarantee secrecy from the moment the vote is encrypted. It cannot guarantee the secrecy of the vote prior to that moment. Neither can a system prevent the secrecy of the vote to be violated in case an elector votes from a PC at home or at work, from a computer at an informal public place or kiosk, or even from a mobile phone. Freedom and non-coercibility can only be fully guaranteed if the material circumstances in which the vote is cast, can be controlled. These ideal material circumstances can be attained when Internet voting is only allowed from official polling places and presumably also when it will be allowed from unofficial public places and kiosks. But when Internet voting will be possible from home or workplace or from a mobile phone, these material circumstances clearly cannot be implemented or enforced. This can give rise to abusive practices: the buying and selling of votes, coercion by family members ('family voting') or by employers or colleagues, etc.

It is to be recommended to enact laws that provide obligatory and enforceable rules with regard to the material circumstances in which a vote has to be cast, and sanctioning the practice of illegitimately influencing a voter.

2.2.2. One Person, One Vote. The universal and equal suffrage is another basic principle of democratic elections: each elector is entitled to only one vote. It also

implies that every vote is counted equally. Naturally there may be no possibility to alter or remove a validly cast vote in the course of the voting process.

The principle entails 4 principles: (1) only legitimate voters can be allowed to vote; (2) each legitimate voter can vote only once; (3) every legitimately cast vote has to be counted once and (4) a legitimately cast vote may not be able to be altered in the course of the voting process.

The first two principles concern authentication, the last two principles refer to security and reliability.

As regards authentication, this can be divided into *physical and digital authentication.*

The first one signifies that the voter is identified, based upon one or more physical characteristics like gender, face, fingerprint, eye-structure, signature, handwriting, DNA-structure, etc.

The latter is performed by using a personal, secret code, which can be a number incorporated in a magnetic card or a chip-card, or a simple letter and/or figure combination, etc. Naturally the voter has to receive the code and the matching password in advance.

This transfer can take place in two ways: *off-line and online.*

Off-line, the code is provided after physical authentication of the voter: based on his physical characteristics, it is controlled that he is indeed the person he claims to be and that the code has not yet come into his hands. In the future, it would be possible for example to provide every citizen, after physical authentication, with an identity card with a chip or magnetic strip built in, containing the personal code (his 'private key'), which can be used for authentication in public and private life, in combination with a secret, personal password. This private key could then also be used for authentication in Internet elections.

The personal identification code can also be provided online. Nevertheless, authentication then is unreliable for it is based on non-verifiable elements. In any case it is essential for the private key to be kept on a safe carrier. A magnetic strip isn't safe enough, because its content can be read too easily. Therefore, the private/public key pair authentication should be used according to the methods and standards of the existing and future Public Key Infrastructures (PKI).

From a legal point of view it is worth mentioning that the law considers a digital signature of equal value to a handwritten signature. This is explicitly provided in Directive 99/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures [5], which states in article 5 that "*Member States shall ensure that advanced electronic signatures, which are based on a qualified certificate and which are created by a secure-signature-creation device, satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data and are admissible as evidence in legal proceedings.*"

Thus there is a tendency to recognise the digital signature technique as a legally valid authentication method.

that an electronic ballot is not forged or modified surreptitiously; (3) *vote privacy*: assuring that no one can find out how any individual voter voted; (4) *vote reliability*: assuring that no Internet ballot can get lost; (5) *non-duplication*: assuring that no voter can vote twice; (6) *defence against denial of service attacks* on vote servers and clients and (7) *defence against malicious code attacks* on vote clients.

2.2.4. Verifiability and Audit Ability of the Voting Process. Voters, independent officers, representatives of the political parties in competition and independent observers – including media reporters – must be able to control polling and tabulation. This could require the individual ballots to be recorded permanently on indelible media to allow for a recount should that be necessary.

The integrity and trustworthiness of a voting system is greatly enhanced by having an audit trail recording each ballot cast. Audit trails with very high integrity can be obtained when the audit trail is created directly by the voter, as with a paper ballot. However, electronic voting systems are indirect. They interpose a layer of mechanism between the voter and the audit trail, risking the possibility that the mechanism is not faithfully capturing the voter's preferences [8].

2.2.5. Voter's Confidence in the Voting System. In order to enhance voters' confidence in the online voting system, it could be recommended to make the source code publicly available, in order for citizens to be able to study the software and verify the reliability and security of the system. On the other hand however, open sources can make the election system more vulnerable to hacking attacks and therefore compromise the security of the system. A solution may be to open the source only to a select group of experts, like for instance the election committee that manages the election and/or independent advisors.

3. Online Voting Systems and Anonymity

How can one guarantee that a vote over the Internet is cast by the legitimate voter while guaranteeing his privacy at the same time? In order for one computer to send data to another – as is the case in any Internet voting system – both computers must know the unique address of the sender and the recipient of the data. This unshakable tenet of the Internet contrasts sharply with the requirement of the secret ballot in elections.

The secrecy of a voter's ballot choice should be preserved and every reasonable technical means should be used to prevent anyone from violating ballot privacy anywhere along the path from the vote up to the election results. It's easy to understand the critical importance of a secret ballot, defined as a way to cast a vote "in such a manner that the person expressing such choice cannot be identified with the choice expressed." A private, anonymous ballot protects the process from votes being bought or sold, and protects you from coercion.

that an electronic ballot is not forged or modified surreptitiously; (3) *vote privacy*: assuring that no one can find out how any individual voter voted; (4) *vote reliability*: assuring that no Internet ballot can get lost; (5) *non-duplication*: assuring that no voter can vote twice; (6) *defence against denial of service attacks* on vote servers and clients and (7) *defence against malicious code attacks* on vote clients.

2.2.4. Verifiability and Audit Ability of the Voting Process. Voters, independent officers, representatives of the political parties in competition and independent observers – including media reporters – must be able to control polling and tabulation. This could require the individual ballots to be recorded permanently on indelible media to allow for a recount should that be necessary.

The integrity and trustworthiness of a voting system is greatly enhanced by having an audit trail recording each ballot cast. Audit trails with very high integrity can be obtained when the audit trail is created directly by the voter, as with a paper ballot. However, electronic voting systems are indirect. They interpose a layer of mechanism between the voter and the audit trail, risking the possibility that the mechanism is not faithfully capturing the voter's preferences [8].

2.2.5. Voter's Confidence in the Voting System. In order to enhance voters' confidence in the online voting system, it could be recommended to make the source code publicly available, in order for citizens to be able to study the software and verify the reliability and security of the system. On the other hand however, open sources can make the election system more vulnerable to hacking attacks and therefore compromise the security of the system. A solution may be to open the source only to a select group of experts, like for instance the election committee that manages the election and/or independent advisors.

3. Online Voting Systems and Anonymity

How can one guarantee that a vote over the Internet is cast by the legitimate voter while guaranteeing his privacy at the same time? In order for one computer to send data to another – as is the case in any Internet voting system – both computers must know the unique address of the sender and the recipient of the data. This unshakable tenet of the Internet contrasts sharply with the requirement of the secret ballot in elections.

The secrecy of a voter's ballot choice should be preserved and every reasonable technical means should be used to prevent anyone from violating ballot privacy anywhere along the path from the vote up to the election results. It's easy to understand the critical importance of a secret ballot, defined as a way to cast a vote "in such a manner that the person expressing such choice cannot be identified with the choice expressed." A private, anonymous ballot protects the process from votes being bought or sold, and protects you from coercion.

A system is *private* [9] if neither the election authority nor anyone else can link any ballot to the voter who cast it and no voter can prove that he/she voted in a particular way.

Home-based electronic voting which, by its very nature, is unsupervised, represents a threat to the core values of freedom and fairness which underlie democratic elections. There can be no guarantee of the freedom from external influence by third parties during the casting of votes at home. This constitutes an inherent risk of any form of remote voting. To face this risk, measures should be taken on the policy and regulatory levels, in order to impose compelling and enforceable measures against coercion and to sanction illicit behaviour. Uncoercibility and the prevention of vote buying and extortion can be ensured by an e-voting system designed so that no voter can prove that he/she voted in a particular way (untraceability on the part of the voter [10]). In democratic elections, the link between the ballot and the voter must be irreversibly severed to ensure that votes are cast freely. Voters must be unable to prove how they voted, in order to reduce the risk of coercion or vote selling. For if voters cannot prove how they voted, buying votes becomes a worthless endeavour in that potential vote buyers would not know what they are buying.

However, academics highlight the need to maintain a paper trail of how each individual voted, in case the votes would need to be counted manually in the event of a recount. The presence of such an audit trail would inevitably entail the tracing back of each individual to their vote, thereby compromising their anonymity. There will always be a trade-off between the two [11]. The e-voting system should be designed in such a way as to make vote control and recount technically feasible, without re-identifying the voters.

A possible solution to the threat of coercion is to develop a publicly accessible infrastructure, in public and controlled physical sites, thus allowing voters to exercise their rights free of the coercion of any third party. This solution however, outweighs the advantage of mobility, in that there are restrictions on the location from which a voter can cast his vote [12]. Immediately after the sending of the ballot to the server and without waiting for feedback from the server, or immediately after the moment that the voter clicks on the 'cancel' button, all records of the vote must be deliberately erased from the voter's computer.

Despite the risks, a lot of people want a home Internet voting solution. The ability to vote from home seems to be very convenient and attractive to Web-connected households, potentially increasing voter turnout for future elections. Although, it would be essential, especially in the first phases of any Internet voting introduction, to retain centralized polling places for those who would not have access to computers otherwise.

Voter anonymity can be achieved by masking the identity of each voter so that no reverse association can be made. However, such an approach makes accountability

much more difficult. One-way hashing functions or even public-key encryption may be useful for providing later verification that a particular vote was actually recorded as cast, but no completely satisfactory scheme exists guaranteeing voter anonymity, consistency of the votes tabulated with respect to those cast and correct results.[6] Any attempt to maintain a bi-directional online association between voter and votes cast is suspect because of the inability to protect such information in this environment [13].

Encryption, through the use of digital signatures and digital certificates, requires a public-key infrastructure (PKI) to identify and authenticate millions of voters. Even with PKI or some other form of security in place, there is no guarantee that a person's vote will remain anonymous. Digital signatures don't solve the anonymity problem. There's still the risk that a vote filed with a digital signature could be tracked and identified by a government authority.

4. Current State of Affairs within the European Union

4.1. Belgium

In Belgium, the first introduction of the possibility to vote electronically, i.e. during the municipal elections of 2000, has given rise to quite a lot of legal claims concerning the lack of transparency of electronic voting. One court claimed electronic voting to be illegal in the context of international law. Although the court admitted that it was not competent to prevent the elections from being held, it ruled that a system in which flaws and fraud can only be detected by the established power at the moment of election and not by an independent authority, violates the rights guaranteed by the International Convention of December 19, 1966 on civil and political rights.

Bearing in mind all the obstacles blocking the way to a well functioning electronic voting system, one could consider having recourse to Internet voting. Voting through optic reading of the paper ballots has been put forward as a way of enhancing the processing of the results, while safeguarding the trust of the voters; however, the system does not tackle the fact that voters need to be present themselves at the polling station. Internet voting, by contrast, can serve as a mobile system in which there are no restrictions (other than the logistical ones) with regard to the location from which a voter can cast his vote.

At the end of February 2003, the Belgian Government decided to expand the possibility of electronic voting over the whole country as from the municipal elections of 2006.

---

[6] The CyberVote project claims to be one of the most innovative and secure systems available. For additional information consult the official website at http://www.eucybervote.org.

4.2. United Kingdom

Voting by mail is the most common form of early or absentee voting. In the UK, postal voting has proven to be a success in terms of improving voter turnout. Postal votes can be obtained on demand as a result of changes introduced by Section 12 and Schedule 4 of the Representation of the People Act 2000, which entered into force on February 16, 2001[7].

During the last couple of years, the UK has expanded its programme for e-voting experiments (in particular voting via the Internet, SMS, touch screen kiosks and touch telephones). The UK Electoral Commission[8] stated in its evaluation report of the electoral pilot experiments conducted in May 2002 that it had not found any evidence of an increased risk of fraud. "However, further testing is clearly deemed to be highly necessary to tease out a number of practical issues, to foster public confidence and to further develop the security of e-voting mechanisms".

The 2003 electoral pilot program was a partnership between the Office of the Deputy Prime Minister, the Office of the E-Envoy, the Electoral Commission and the Local Government Association (LGA). The project enabled over 1.5 million voters to cast their vote electronically by phone, SMS, and the Internet. An additional channel was available to voters because for the first time, voting was possible using interactive digital television (iDTV). During these experiments, voters were able to vote before the normal polling day. Instead of a polling card, they received IDs to prevent multiple voting and they were provided with information packs explaining how the system operated. Four municipal authorities did not even offer the traditional voting methods, so that voters who didn't dispose of the e-voting equipment had to resort to postal voting.

Despite some minor problems, the operational problems were overcome and the potential vulnerabilities arising from the procurement process did not cause material problems during the election period. There is clearly a balance to be obtained between security, convenience and accessibility. In general, the election was carried out competently, meeting a good commercial standard. However, the risk of malicious attacks was low as the systems were recently developed, the implementation varied widely across the different pilots and the relative uptake of electronic voting is still less than traditional methods. Therefore, in the Electoral Commission's opinion, the motivation and capacity of potential attackers was likely to be low. Evidently, as the e-voting programme will progress towards the Government's objectives, the threats will increase and a number of significant issues will have to be addressed accordingly.

[7] http://www.hmso.gov.uk/acts/acts2000/20000002.htm.
[8] http://www.electoralcommission.org.uk/about-us/researchpub.cfm.

4.3. Switzerland

Under the impulse of the federal Government, three cantons – Neuchâtel, Zürich and Geneva –took their first steps in the area of online democratic elections in 2002.[9]

Whereas Geneva and Neuchâtel tailored their systems exclusively to the personal computer, Zürich took into account that, in the future, citizens may rely more on mobile phones, personal digital assistants or other mobile devices. Consequently, Zürich envisaged a polling system in which all problems relating to reliability, security, encryption and privacy are solved for a very wide range of different hardware configurations, operating platforms, software applications and transmission protocols.

In March 2001, the Geneva State Council officially launched the *'Geneva Internet Voting System'* [10]. In a comparative international perspective, the current Internet voting project in the Canton of Geneva stands out as one of the few serious attempts to implement binding governmental voting procedures. The aim of the project was to offer an additional way of casting a ballot. The Internet Voting System didn't intend to replace the existing ballot forms – the traditional ballot box or postal voting – at least not in the near future. Recently, the state of Geneva has taken the e-voting project interoperability and accessibility to the next level through the integration of biometric and voice recognition technology.

A recent Internet voting experiment during a referendum in Anières (Geneva) in January 2003 turned out very successful. However, the project strictly focused on voting on yes-no issues so that complications in respect of electoral procedures have not been dealt with.

4.4. Estonia

In Spring 2001, the Minister of Justice of Estonia proposed the introduction of electronic voting in future elections.[11] Since voting is not compulsory in Estonia, the government hopes to attract greater participation in elections and political debates by this move to online voting, especially among younger people. According to the plans, citizens will be allowed to register as e-voters and sign their ballots electronically using a digital signature, which would enable voting via Internet at home. However, Internet voting will not eliminate traditional voting; it is merely an additional way of voting.

The current Election Act provides for the possibility to vote electronically at the latest in the year 2005, on the one condition that all crucial technical issues are solved by that time. The focus is mostly on safeguarding against fraud. Although security is a major concern, it is believed that a combination of digital signatures and smart card

---

[9] http://socio.ch/intcom/t_hgeser12.htm.
[10] www.geneve.ch/chancellerie/E-Government/e-voting.html.
[11] http://www.vm.ee/eng/kat_175/2972.html.

identification will be sufficient to eliminate fraud. In order to vote electronically, voters need to have a digital signature certificate, which is programmed in their electronic ID card. This card was introduced in 2002. Internet voting would take place only on advance polling days. This will be easy, as many Estonians are already used to voting during advance polling days.

4.5. Conclusion

This short overview demonstrates that in the near future and provided that the scheduled trial experiments are successful, Internet voting will not be limited to certain non-binding or informal local elections, but that it will be tested during some major elections. There is no question about it that the results of such major experiments will be of crucial importance with a view to the use of the Internet as a means of voting in the near future.

Conclusion

Implementing an online voting system offers a lot of advantages. Firstly, it may increase voter turnout by making the elections more convenient and more accessible to disabled voter. Secondly, online voting can be made more interactive and relevant by allowing voters to see photos and statements by the candidates next to the ballot. Finally, electronic voting can bring the population closer to the concept of a 'direct democracy', wherein the citizens themselves can participate more actively in the creation of laws [14].

The right to vote is only one part of the democratic process, but it remains a civil right deeply embedded in constitutions and is considered to be one of the primary foundations of democracy. Hence, e-voting is not like a common electronic transaction. An e-voting procedure will only be acceptable under the condition that it safeguards the constitutional principles associated with the voting process, as there is equality, freedom, secrecy, transparency and accountability.

It is important to realize that submitting one's identity for purposes of assuring voting eligibility can easily serve as a way to identify what vote an individual has cast. In addition, the vote-recording process is invisible to the voter; thus there is no reliable way of ensuring that propriety is kept. By their very nature, electronic operations on data are invisible to the user, and experts in the field confirm that the technology simply does not exist to authenticate transactions while ensuring total anonymity of the voter [15]. Therefore, even if a voting program states that it keeps identification information separate from voting information, an individual voter would have no way to confirm this. The difficulty lies in convincing voters that their privacy is maintained at all times.

To this end, the public must be kept apprised of the manner by which the Internet is protected from outside influences, including national and international hackers as well

as individual voters who might try to cast more than one ballot. Additionally, it is imperative that all voters are assured that their right to a secret ballot is protected and guarded by government officials who themselves are kept aware of who has voted, but purposely are kept ignorant of how individuals voted. This is the fine line that those who administer Internet voting must walk – audits must be possible, fraud must be impossible and the secrecy of ballots must be ensured at all times.

The legal framework should provide for ballot security, while at the same time ensuring that no individual ballot can be identified as being marked by a specific voter [16].

For the moment it seems unlikely for the anonymity of the vote to be fully guaranteed in a remote (online) electronic voting system, in which voters would be allowed to vote from any PC connected to the network (a PC at home or work for instance). While electronic voting from home should perhaps forever remain too risky a fantasy, electronic poll-site voting may provide, even in the near term, worthwhile improvements to paper-based voting technologies. A remote online voting system requires distance authentication of the voter and it does not allow control as to the circumstances in which the vote has been cast.

Today, no sufficient technical solutions exist for the situation in which the secrecy of the vote cannot be guaranteed in a remote online voting system, unless measures are taken on policy level and laws are drafted and enacted which impose compelling and enforceable measures and which sanction illicit behaviour.

References

1. California Secretary of State, *California Internet Voting Task Force Report,* January 2000 (USA) – http://www.ss.ca.gov/executive/ivote
2. R. RIVEST, "Electronic voting", http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf
3. Internet Policy Institute, "Report of the national workshop on Internet voting: issues and research agenda", 2001, http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf
4. L. MITROU, D. GRITZALIS and S. KATSIKAS, "Revisiting legal and regulatory requirements for secure e-voting", 2002, http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/evote_paper_SEC_2002_2.doc
5. Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, *O.J. L.* 013, 19 January 2001
6. R. RIVEST, "Electronic voting", http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf
7. California Secretary of State, *California Internet Voting Task Force Report,* January 2000 (USA) – http://www.ss.ca.gov/executive/ivote

8. R. RIVEST, "Electronic voting", http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf.
9. L. CRANOR, "Electronic Voting, computerized polls may save money, protect privacy", ACM Crossroads Student Magazine, April 1996, http//www.acm.org/crossroads/xrds2-4/voting.html.
10. L. MITROU, D. GRITZALIS and S. KATSIKAS, "Revisiting legal and regulatory requirements for secure e-voting", 2002; http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/evote_paper_SEC_2002_2.doc
11. "E-voting security study, issue 1.2", 2002, http://www.edemocracy.gov.uk/library/papers/study.pdf
12. L. CRANOR and R. CYTRON, "Sensus: a security-conscious electronic polling system for the Internet", 1997, http://lorrie.cranor.org/pubs/hicss/.
13. P. NEUMANN, "Security criteria for electronic voting", 1993, http://www.csl.sri.com/users/neumann/ncs93.html
14. University of Maryland, Towson University, "Electronic voting research project", http://www.bsos.umd.edu/gvpt/lawonline/journals/lolj2/LOLPAPER1a.doc.
15. C. LAVIN, "Internet voting and preserving anonymity.", *San Francisco Chronicle*, April 17, 2000, A23.
16. Office of the Deputy Prime Minister, "Implementation of electronic voting in the UK, a report addressing the legal issues", http://www.local-regions.odpm.gov.uk/egov/e-voting/01/03.htm