Internet Voting

Excerpts from

Technology and Administration in Election Procedure

Final Report from the Election Technique 2000 Commission

Stockholm, Swedish Government Official Reports, SOU 2000:125 (Ministry of Justice)

Contents of the full report[1]

[1] The full report is available in Swedish at http://www.justitie.regeringen.se/propositionermm/sou/pdf/sou2000_125.pdf

5 Internet Voting

Summary of the Commission's conclusions

The point of departure is that a system of electronic voting ('e-voting') via the Internet must fulfil the following five basic requirements:

- Only people eligible to vote should be able to vote.
- It should be possible to use one's vote only once.
- Ballots should be absolutely secret.
- It should not be possible for a vote cast to be changed by anyone else.
- The system should ensure correct tallying of votes at all levels (voting district, constituency and area).

The Commission presents an e-voting system for Internet (online) voting that should be capable of fulfilling these requirements. Before it is tested in an election, however, extensive trials should be carried out. Only after such trials can a final decision be taken as to whether the procedure is applicable in a real election.

5.1 Some starting points

One basic precondition for e-elections must be the feasibility of implementing the voting under such conditions that the principles underpinning the electoral system are not disregarded. Accordingly, the system must be at least as secure as corresponding traditional voting procedures. Another precondition is that the e-voting procedure must be simple and function smoothly for the voters. Its overall purpose is to enhance accessibility to voters.

The present form of voting in general elections is founded entirely on paper-based and largely manual voting procedures. New technology with advanced vote-client machines (computer terminals used for voting) for e-elections may entail several advantages. It may, as mentioned above, enhance the voters' scope for participating in the election. It also creates scope for more rapid tallying of votes and distribution of seats. This also enables the electoral administration to promptly announce the election results to a broader circle. The risk of error in vote-tallying can also be largely eliminated.

The new technology also entails disadvantages that must be considered. One is the difficulty of guaranteeing ballot secrecy with absolute certainty. Another is the question of how to guarantee the reliability of the system, i.e. that the system will in all situations function in the manner in which it is meant to function. Another disadvantage is the expense of development and operation. All in all, then, the primary considerations are security and reliability.

5.2 What requirements should be imposed on the procedure?

The Democracy Commission has, on several occasions, dealt with the issue of electronic elections and the requirements that should be imposed on such a procedure.

The Democracy Commission's report No. 16 (SOU 1999:12), *Electronic Democracy* (in Swedish) by Anders R. Olsson, maintains that Sweden's use of a paper-based, mainly manual voting procedure is not due to technical backwardness. Instead, according to Olsson, the reason is that an IT solution is far too vulnerable in purely physical terms. Saboteurs could cause disruption in telecoms and the power supply. Another reason, according to Olsson, is protection for ballot secrecy, i.e. the need to prevent any outsider from being able to find out how one has voted. This means, too, that certain transactions in a voting system cannot be revised after the event. Otherwise, a guarantee for citizens' confidence in this type of system lies in the fact that the computer programs that make the decisions are public and can be tested with their own data.

In its report *A Sustainable Democracy* (in Swedish, SOU 2000:1), p. 188, the Democracy Commission considers that increased use of IT in voting will probably enhance accessibility to, for example, the groups of young people where electoral participation should be boosted. But as long as IT is not universally accessible there is, however, according to the Democracy Commission, no reason to believe that voters in a weak socioeconomic position would increase their electoral participation as a result of such electoral procedure. There is also a risk of the procedure tending to become a mere expression of public opinion on election day, and to lose the gravity, dignity and symbolic significance of the traditional act of voting. The problem that must be solved first, according to the Commission, is that of how voters should authenticate their identity, to render electoral fraud impossible without ballot secrecy simultaneously being lost. Other problems are how it can be guaranteed that no one is subjected to unauthorised influence at the actual time of voting, or that no unauthorised person casts a vote. In view of the above-mentioned problems, the Democracy Commission has proposed that trials of Internet voting should be carried out in a municipality or in connection with school elections.

Corresponding issues have also been dealt with in detail in an American survey, *A Report on the Feasibility of Internet Voting*, issued by the California Internet Voting Task Force in January 2000.

Below, the Commission considers which basic requirements should apply to an electronic Internet voting procedure.

The Commission's basic requirements

According to the Commission, the premises are as follows:

- The electoral system must fulfil stringent reliability requirements.
- There must be guarantees that the election takes place in such a manner as to safeguard ballot secrecy.
- The electoral procedure must be simple and function smoothly.

Consequently, an electronic voting system via the Internet must fulfil the following five basic requirements:

- Only people eligible to vote should be able to vote.
- It should be possible to use one's vote only once.
- Ballots should be absolutely secret.
- It should not be possible for a vote cast to be changed by anyone else.
- The system should ensure correct tallying of votes at all levels (voting district, constituency and area).

Other circumstances that may need to be taken into account in such a system are safeguards for the voters' personal integrity and means of preventing the sale of votes. The first issue relates to the setting in which voting takes place, for example in a venue that is not subject to surveillance by the polling administration. The second issue relates to voters' ability to verify afterwards how the system has dealt with their votes.

Identification

To fulfil the first-mentioned requirement that only people eligible to vote should be able to do so, secure online identification of the voters must be feasible. This presupposes, first, that it is practicable to require ID particulars from voters when they log on and, secondly, that each voter has a unique, personal password.

At present, the election database contains the national civic registration number of everyone who is included in the electoral register. In an Internet voting system, the electoral register needs supplementing with the voter's personal password or code, to permit reliable identification.

One alternative that may be considered is whether, as in Finland, to introduce a citizen's smart card on which the holder's ID particulars are stored on a microchip in a plastic card. Introducing such a card would permit the problem of identification (authentication) in online voting to be solved. This presupposes, however, that voters have card scanners connected to their home computers, and this requirement currently restricts many people's scope to vote online using their home computers. In this context, the Commission wishes to point out that other techniques of identification exist as well, but these also entail specific requirements concerning hardware and the software installed on the user's computer. The Commission's conclusion is therefore that the eligibility requirement is a problem at present, but not necessarily so in the long term.

Only one vote

Fulfilling the second requirement, that one should be able to vote only once, is unlikely to entail a problem. The system has information on all those who are eligible to vote, and when they do so their votes are — just as in the present-day manual procedure — checked against the electronic electoral register. According to which arrangement is recommended, this means either that the second vote does not count, since it cannot be checked against the electoral register, or that counts as a revised vote, whereupon the first vote cast is disregarded.

Ballot secrecy

The third requirement, that ballots should be absolutely secret, gives rise to thorny problems in e-elections. To fulfil the first two requirements, voters must provide information about themselves (i.e. identify themselves) to enable the system, first, to determine whether they are eligible to vote and, secondly, to check that they have not already used this right to vote. Here, there is what in these contexts is often called a 'package problem', i.e. the connection between identity and vote. Accordingly, in an e-voting system it must not be technically feasible for anyone to open the 'package' and view both particulars simultaneously.

According to the current rules in the Election Act, it is possible to revise one's vote in advance voting, but not in voting at a polling station on election day. Accordingly, information on the voters' identity and votes must in any case be kept together until the voting is concluded at 8 p.m. on election day.

Safeguarding votes cast

The fourth requirement, that no unauthorised person should be able to change another person's vote, calls for the 'package' to be safeguarded during its transfer from the voter's computer to the e-voting system. At present, various techniques are available for information packaging, encryption, etc and these techniques, in the Commission's estimation, fulfil reasonable requirements for a secure system.

Trustworthiness and legitimacy

The fifth requirement, that the system should be perceived as trustworthy and should impart legitimacy to the election results, imposes special requirements in terms of permitting a revision of the system to be carried out where necessary. In the paper-based manual system in use at present it is possible, in any case theoretically, to trace all the results of a parliamentary election, for example, by recounting the votes — thus showing that the result reported is also correct. In e-elections, in the Commission's estimation, interest in checking election results may be even stronger, especially in view of known security risks such as hackers.

For the system to be perceived as trustworthy, the voters must have a sound understanding of its structure and functioning. This imposes special requirements on the educational presentation of the system. But according to the Commission, it must also be possible for voters to trace (audit) the votes they have themselves cast, and thus see for themselves whether the system has dealt with these votes in the manner intended.

5.3 Experience in other countries

In questionnaires addressed to other EU member countries and also Iceland, Norway and Switzerland, the Commission has asked, first, whether Internet voting has been used in any elections and, if so, what the experience of its use has been and, secondly, whether there are plans to hold an election by such means. The questionnaire responses are reported in *Annex 3* to the report. Summing up, none of the countries asked were found to have implemented Internet voting in any election or referendum. In some countries, trials of e-voting have been carried out on a limited scale, but these have not involved use of the Internet. In several countries, including Ireland and The Netherlands, however, there are plans for such e-voting trials to be carried out within the fairly near future.

In Ireland, the Government has decided in principle to introduce e-elections and e-referenda. Under this decision, voting is to take place at a polling station by means of 'touch-screen' technology. The votes cast will be stored on the hard disk in the vote-client machine which, after voting is completed, will be transmitted to a common vote-server data centre (VSDC) for tallying.

In The Netherlands, the intention is to implement elections with e-voting in the year 2003. Trials have been under way since 1995. Provisions permitting voting with magnetic cards are to be inserted in the current election law.

In Norway, a government commission of inquiry has announced that it intends, in its proposal for a new election law, to include a provision enabling trials of Internet voting to be carried out.

E-voting trials

Below, the Commission reports on some of the most important trials of e-voting carried out to date (see also *Electronic Voting Experiment*, a report by Aldo D'Ambrosio Gomáriz, Generalitat de Catalunya, Spain, May 1999). It should be emphasised that no trials of Internet voting have been held.

In Belgium, e-voting has been carried out in local elections since 1991. The first e-election was limited to the canton of Verlaine, and e-voting was then successively extended to more and more cantons. In the latest local elections, in 2000, it was possible to vote electronically in all the cantons. The Belgian system involves a touch screen. The voter receives a smart (magnetic) card from the polling official, and then places it in the card scanner of the machine. The voter then points and clicks to select his or her chosen party, list and candidate, and an image of the resulting ballot then appears on the screen. Thereafter, the voter can confirm the selection. The vote is stored electronically in the vote-client machine and on the magnetic card — on the latter, in order to be stored separately for security reasons. In some cases, the voting particulars have been recorded on floppy disks and transported to the venue for the central count.

In France, two local trials of e-voting have been carried out: one in connection with elections to the European Parliament in 1994 and one in connection with the presidential election of 1995.

In Spain, e-voting has been implemented on a trial basis in connection with the Catalonian provincial election in 1995. What happened was that, after completion of the regular voting procedure, the voters who wished to do so were able to join in an e-voting trial in another part of the polling station. Electronic cards and a personal computer with a scanner pen were used. Each vote was stored on the card, which the voter then placed in a ballot box. In a second trial, carried out in Catalonia in 1997, two different systems were used. In one, the ballot box had a card scanner in the slot. In the other, votes were collected digitally in the vote-client machine and the cards were used as back-up.

In Japan, in April 1999, an e-voting pilot project was implemented in connection with the elections in Kawaguchi. Slightly over 360,000 people, in 78 electoral districts, were eligible to vote in these elections. In 11 of the districts, with a total of 55,000 people eligible to vote, trials of e-voting and electronic vote-tallying were arranged. These trials were carried out parallel to the ordinary elections, purely for testing purposes. First the voters cast their votes in the ordinary election; after that, they were invited to join the trial. The trial premises were adjacent to the regular polling station.

The system tested in this trial was based on its capacity for reception and storage of votes, and subsequent tallying to obtain the election result. Every polling station was equipped with containers for magnetic cards, voting terminals and voting booths, and also manned with administrative staff. The terminals in the polling stations were connected to a local network, enabling all the votes from all the terminals to be collected and subsequently counted. The counting procedure was that the data were stored on floppy disks that were then transported elsewhere for a central count.

In voting, the voters first showed their voting cards to the polling official. The latter then gave each voter a magnetic card from the card container and showed him or her to a free booth. The voting terminal used had a touch screen, and voters were able to select their preferred lists or candidates and then cast their votes. When the voters left the booths, they then dropped their magnetic cards into a ballot box.

5.4 A system of e-elections that should be amenable to testing

As pointed out by the Commission, there are several problems associated with e-voting systems, especially if the voters are to be able to vote not only in their local polling stations, using computers provided and controlled by the polling authority, but also at venues where the authority cannot supervise the voting, and using computers similarly outside the authority's control, e.g. in voters' homes or at their workplaces. Thus, numerous requirements must be fulfilled. An e-voting system must be capable of self-protection in an insecure environment. The system must also be compatible with the program modules and operative systems used by those who vote.

In this matter, the Commission has co-operated closely with a research group at the Swedish Institute of Computer Science (SICS), for the purpose of presenting an e-voting system that fulfils the basic requirements recommended by the Commission for such a system. In the traditional, paper-based, manual election system, these basic requirements are satisfied by physical barriers. It is, for example, virtually impossible for a person to vote more than once in the same polling station without being recognised. In addition, there is the geographical spread of polling stations. Fraud on a large scale is thereby ruled out in practice. In an electronic environment, this type of physical barrier must be superseded by other, electronic barriers.

Another problem is that of mediating the right to vote in the election to those eligible to vote. A solution that appears suitable is to use existing electronic infrastructure, e.g. smart cards for identification and web scanners as tools for the voting.

Detailed description of an electronic voting system

The following is a somewhat simplified explanation of how an e-voting system can be constructed to fulfil the five basic requirements. The system consists of

- voters, i.e. people eligible to vote
- an electronic ballot box that collects the votes
- two or more scramblers that render the voters anonymous through encryption, and
- a vote tallier that compiles the election result.

Voting and identification

Every vote, x, is triple-encrypted in the above example. The triple-encrypted vote is denoted x’’’. Every vote is thus encrypted once per scrambler. The voter then submits a pair (name and x’’’) with his or her name and the encrypted vote to the electronic ballot box. To prevent fraud, the pair submitted is digitally signed by the voter.

When the election is completed, the electronic ballot box generates a list of valid votes by checking the signatures, i.e. by comparing every pair submitted (name, x’’’) with the electoral register. The precondition for a person’s eligibility to vote in the election is that his or name is included in the electoral register. In this system, it is possible for anyone to check that this is being done in a correct way.

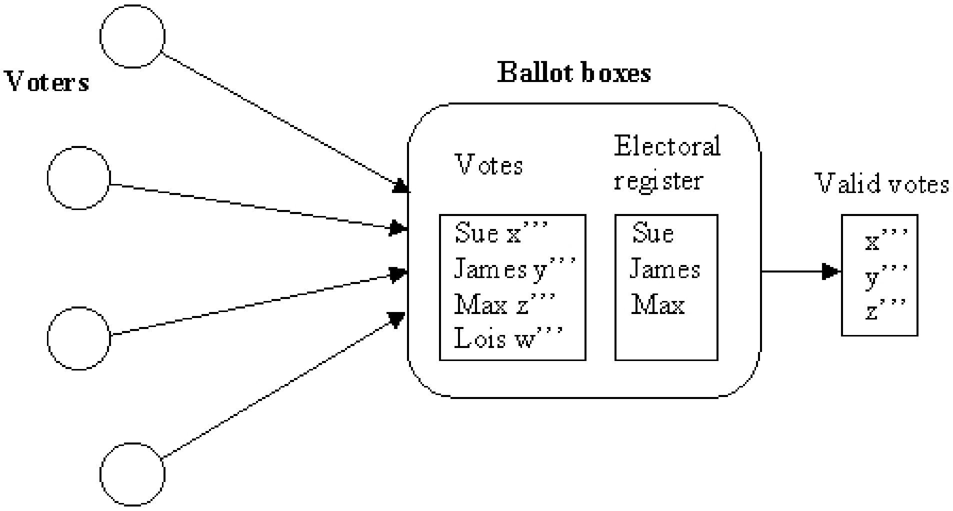

Figure 1. Casting one’s vote. The symbol x’’’ means that the vote is x triple-encrypted.

The system permits revision of one’s vote. If people who have voted change their minds and wish to change their votes, this is fully possible by submitting a new pair (name, x’’’) subsequently. Of the pair received by the system, only the last ones received are registered by the ballot box.

Scrambling

To make it impossible to link a vote with the voter’s identity, the votes cast must be ‘scrambled’ in an anonymisation process. The valid votes are submitted as input data to the first scrambler. Each scrambler except the last issues its output data in the form of input data for the next scrambler (see Figure 2). Each scrambler partially decrypts each vote and then lists the decrypted votes in a random order.

Revealing how a particular person has voted would require all the scramblers to work together. No one scrambler alone can decrypt votes or determine how they have been converted. Responsibility for the scramblers should therefore be divided between several independent bodies. There are several conceivable options.

Vote-counting

The last scrambler, S3, generates a list of decrypted votes, i.e. votes in plain text. It is then possible for anyone to summarise the result of the election (see Figure 2 below).

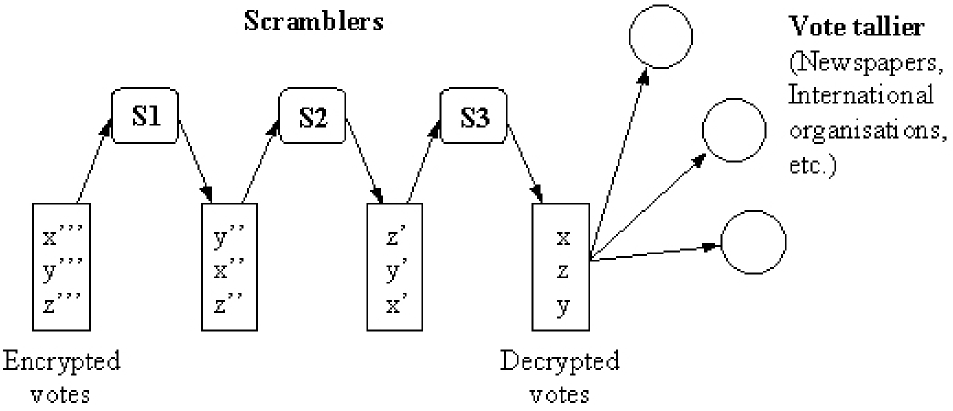

Figure 2. Anonymisation and vote-tallying.

Control

To reveal fraud, the system allows the correctness of every stage to be proved retroactively. The electronic ballot box and scramblers publish their input and output data publicly. On the basis of these particulars, every scrambler can prove to anyone wishing to have the result substantiated that fraud has not occurred. In principle, it suffices for voters to trust at least one scrambler. The choice of organisation to run the various scramblers will therefore be extremely important.

If voters do not trust any scrambler, they can personally check that the votes they have cast have been tallied correctly, by following their votes through the voting system. This is possible since no intermediate results are secret in this system. The voters can themselves subsequently generate their own intermediate results and check whether these are included in the lists concerned produced by the various scramblers. However, the last-mentioned control option means that the system becomes open to the sale of votes. All the voters can simply prove to an outsider how they have voted by revealing all their intermediate results.

5.5 Need for pilot projects

The Commission's viewpoint is — and this should be particularly emphasised — that before Internet e-voting is tried in an election, large-scale trials must be implemented. Only after pilot projects of this kind can a final decision be taken on whether the procedure is applicable in a real election.

In elections today, the assumption is that voting in a polling station on election day should be the primary option. Introducing Internet voting via the voter's own computer may come to change this picture of election procedure. In this context, the Democracy Commission has particularly pointed out that an electronic voting procedure may result in the act of voting tending to be an expression of public opinion on election day, and losing the gravity, dignity and symbolic importance of the traditional act of voting. Security and integrity issues are also highly significant in this context. It should, however, be possible to resolve the latter issues — unlike the first-mentioned issue — without any large-scale pilot project. Before an e-voting procedure is used in a real election it is therefore, in the Commission's estimation, very important to be able to carry out an evaluation of how this form of voting affects voters' perception of the act of voting. Given these considerations it is, according to the Commission, appropriate to first test the procedure in a nationwide school election for pupils at upper-secondary school and in the ninth (last) year of compulsory school. A school election of this kind would involve around 400,000 pupils.

During its inquiry, the Commission and the election unit at the National Tax Board jointly took the initiative in arranging a test of the e-voting system in the school election of 2002. In a test election of this kind documentation could, for example, be obtained for an assessment of the question of how voters perceive the act of voting.

5.6 Multi-stage procedure

The technical threats to an e-voting procedure that relate mainly to the issues of system security, protection for personal integrity and ballot secrecy must not be underestimated. The risk of a computer virus or of an unauthorised person gaining access to a home or workplace computer used in voting is not negligible. Although protection against such attacks exists, they may ultimately result in the voter's vote being disallowed.

The Commission considers that an e-voting procedure should be introduced in stages, along the following lines:

- in the polling station in the electoral district where the voter is included in the electoral register
- in any polling station

- from computers provided by the polling administration at venues where there is no supervision by staff from the polling administration, and
- from any computer whatsoever with an Internet connection.

One of the more intractable problems is which means of identification voters should use in order to be allowed to vote. As long as this issue has not been resolved in a practical and acceptable way e-voting must, in the Commission's view, take place in polling stations or other voting venues where the vote server (recipient) is responsible for this supervision. Taking into account miscellaneous technical problems and the existing security requirements as well, the Commission deems that an electronic Internet voting procedure must initially be tried out in polling stations under the surveillance of polling officials. This would also ensure that the polling administration is in control not only of the voting system as such, but also of the computers used in voting.

A gradual introduction of this kind also makes it possible, over time, to determine by testing which technology should be used for such purposes as authenticating the identity of the voter, ensuring the reliability of the procedure and safeguarding ballot secrecy.

Stage 1: Internet voting in the voter's polling station

A computer for Internet voting, placed in the polling station, supplements or supersedes voting with traditional paper ballots. The polling officials check the voters' identity in the usual way and ensure that they have access to electronic ballots. The electronic ballots are transmitted via the Internet to an electronic ballot box and counted. At this stage, all voters wishing to vote online must do so at their own local polling stations.

Stage 2: Internet voting in any polling venue whatsoever

The same conditions apply as in stage 1, with the exception that the voters are allowed in this stage to vote online in any polling venue whatsoever in the country. The computers used for Internet voting are owned, maintained and protected by the polling administration.

Stage 3: Internet voting from public computers

This stage presupposes that the voter has received from the polling administration a unique password or a unique digital signature. The voter is permitted to vote from computers provided by the polling administration, without their being required to be placed in a polling station under the supervision of staff from the polling administration. This is feasible because the voter has received a password or a digital signature. No physical verification of the voter's identity is then necessary.

Stage 4: Internet voting from any computer whatsoever

The same conditions apply as in stage 3, with the exception that the voters are permitted to vote from their own computers, provided that operative systems and web browsers are protected from sabotage.