

Policy on e-voting and counting

This paper sets out the Electoral Reform Society's current position on electronic voting in public elections. It is a position which will from time to time be reviewed in the light of further technological innovation and electoral experience.

This paper is not concerned with private elections in which the electorate might be widely dispersed and the use of a polling booth and ballot box not a realistic option. We recognise that in such elections the risks inherent in electronic voting, while not absent, are unlikely to be as acute as in elections in which all, or most, citizens in a geographic area will be entitled to vote.

Over no more than two decades, electronic technologies have revolutionised the way we communicate and access information. There are many ways in which these technologies can enhance our democracy: for example, they allow us to follow the proceedings of parliament, they give us immediate access to many government documents, they facilitate consultations and communications between elected representatives and their constituents, and at times of election they are increasingly used by candidates to present their views to electors. All of these developments are to be welcomed.

The use of electronic technologies in voting, however, is another matter. Voting, unlike, say, the purchase of a book from Amazon, requires that the voter can be identified as someone entitled to vote, that the vote is recorded without anyone other than the voter knowing for whom it has been cast, and that the voting process is secure in that the votes cast and their totals cannot be altered by any who might wish to fraudulently influence the outcome of an election. Unlike an Amazon purchase, a voter cannot return his 'purchase' and a refund made if things go wrong.

E-voting can take many forms, each with their own risks and potentials. Here we consider:

1. e-counting: in which voters mark paper ballots but the ballot are counted and results computed electronically;
2. machine voting at a polling station, e.g. by touch-screen device;
3. remote voting by the internet, text messaging or telephone.

E-counting of ballot papers

The use of technology to read and count paper ballots may be seen as a logical development of our traditional form of voting. Hand-counting can be a slow process in large or complex elections and modern scanning equipment can be more accurate than the sorting and counting of votes by electoral staff.

E-counting does not affect the experience of the voter who must complete a ballot form in the traditional way. There is therefore no reason to assume that it will lead to higher turnouts (although turnouts might be temporarily increased by publicity surrounding pilots of these new methods). The advantages of e-counting lie in the speed, and possibly in the accuracy, of the count. Cost advantages have yet to be demonstrated.

E-counting has clear advantages for STV elections where the calculation of transfers, etc. can be done by computer rather than by the physical manipulation of ballot papers, and for simultaneous elections involving a considerable amount of computation.

There are two methods to be considered:

1. Elections in which ballot papers are collected and at the close of the poll, taken (if necessary) to a central counting centre where they are put through scanners which record the votes which are then totalled by computer;
2. Elections in which votes are scanned at the time they are cast, often with the scanner mounted on top of the ballot box.

Method (2) may lead to a faster count and has the advantage that the scanner can detect an incorrectly completed ballot form (or one completed in a manner than cannot be read by the scanner) and return it to the voter for amendment, thereby reducing the number of spoiled ballots (a particular advantage with STV elections). However, on the downside:

- it requires electronic equipment at every polling station adding to the problems of security and of dealing with technical failures;
- it requires an electronic storage device (a card or disk) to be removed from the scanner at the close of the poll and transferred to a central computer which will read it and perform the count – an additional stage which offers greater opportunity for machine error and for fraud.

However, whichever method is used, concerns arise over a possible loss of transparency. The concern here is not faults in the technology, which are likely to be rare and not biased in favour of one candidate or another, but that the equipment might have been tampered with in some way to fraudulently switch votes between candidates or to adjust totals.

If e-counting is to be used there should therefore be procedures to allow candidates and their agents to satisfy themselves that the equipment is operating as it should. Measures to reduce the risks of fraud should include:

- Allowing candidates and agents to sample ballot papers and obtain information on how the equipment recorded the votes. (This is not, however, a complete safeguard as a skilful fraudster in charge of the equipment could switch equipment setting to alter the programming as required.)
- Allowing candidates and agents to test machines before, during or after counts by running samples of ballot papers and comparing results with the known results of the sample. Again, not a complete safeguard for reasons given above.
- Using open-source software or making copies of the software available to candidates and their agents so that they can satisfy themselves that it accurately counts votes according to the rules of the electoral system.

With e-counting of ballot papers, there is always the fallback of a manual recount if candidates or their agents suspect that the equipment has malfunctioned or for some other reason has not performed a true count. However, when ballot papers have been fed into equipment at speed, it is possible that equipment that has been tampered with will produce a wrong result without candidates having any reason for suspicion. There is therefore a case for a requirement that a sample of votes should be checked manually (as is done in some states of the US).

Machine voting at a polling station

Here the voter votes using a machine, generally a touch-screen device. This method of voting has been used in many countries. It has the advantage of recording the vote directly without errors that might arise in scanning, and of being able to detect an incorrectly completed ballot paper and give the voter an opportunity to revise it.

In the US, Ireland and the Netherlands, however, this form of technology has given rise to serious security concerns. The problem is that the voter relies on the machine – a black box whose workings the voter cannot see – to correctly record the vote and allocate it to the chosen candidate. The risk is that the machine might have a fault or have been tampered with in a way that records a different vote from that entered by the voter, or does not produce the correct total.

To minimise the risk of fraud, voting machines should produce voter verifiable audit trails. Rather than the voter completing a ballot paper, the machine should produce a ballot paper which the voter verifies and then puts in a ballot box. Should there be a dispute over the result, the paper ballots should be regarded as the definitive votes rather than those recorded on the machines.

Additionally, there should be safeguards equivalent to those described for e-counting.

Internet, text and telephone voting

These forms of voting maximise convenience as the voter can vote from home or office at a time of their choosing, and even voters who are away from home can vote without the need for an absent ballot. Internet voting also has the advantage that while on-line voters can be offered links to the websites of candidates so that they can look at candidates' statements at the time of voting, leading to more informed choices. It has also been argued that internet voting might be more attractive to younger voters, accustomed to using the internet but not to voting at a polling station.

However, internet and telephone voting pose the greatest security risks. The risks fall into two categories:

- Quite apart from concerns that the equipment might have been tampered with by unscrupulous operators, the system is vulnerable to hackers who may plant viruses or corrupt the system in other ways in order to, for example, switch votes from one candidate to another without the voter being aware, alter the totals and hence the result, or simply enjoy the power of disrupting an election. Abuses that involve switching votes or adjusting totals could be very difficult to detect as there is no physical record of the votes that have been cast.
- This form of voting suffers from the problems of remote voting in general. When votes are cast outside a polling station the secrecy of the ballot cannot be assured and there can be no guarantee that the elector did not suffer intimidation or was offered a bribe while voting. Moreover, there is the risk that PIN numbers sent to electors might fall into the wrong hands and the vote be cast by a person other than the person to whom the vote was issued. A change to individual voter registration with personal identifiers held by electoral registration officers (as is being considered for postal voting) would make impersonation more difficult, but

Internet voting can be made more secure by restricting polling to kiosks that might be located in shopping centres, etc, and on a closed system (i.e. not on the open internet), but this seriously reduces the advantage of convenience.

Thus the benefits of internet, text and telephone voting and its potential attractiveness to younger voters comes at the cost of increased vulnerability to attacks on the system, fraud and other forms of malpractice. We need to consider whether the one might justify the other. Low turnout elections cannot be guaranteed to produce representative outcomes, whatever electoral system is used, and if the use of internet, text and telephone voting were to significantly increase turnouts then it might be argued that the increased risks are an acceptable price to pay. However, there are two counter-arguments:

1. Experience in the UK suggests that these voting methods do not significantly increase turnouts (this experience is, however, limited, and as more people become aware of alternatives to voting at a polling station this might change).
2. Changes in voting methods is not the only route to higher turnouts. Turnouts are not low because voting has become more difficult, but because electors have little faith in the efficacy of their votes – they do not sense that their votes will make a difference to the outcome, and they do not believe that who wins will have much impact on their prosperity, security or well-being. A reform of the voting system is likely encourage participation in elections without the risks associated with internet and related methods of voting.

In conclusion:

The Electoral Reform Society therefore believes that for public elections:

1. The electronic counting of votes cast at a polling station, whether cast by a paper ballot or through an electronic device, is an acceptable way of increasing the speed, and possibly the accuracy, of counts provided that sufficient steps are taken to guard against attempts to subvert the election and to give candidates and their agents opportunities to verify the accuracy of the count.
2. Where votes are cast at a polling station electronically, the equipment should produce a voter verifiable paper record of the vote. Where there is doubt over the outcome of an election, the paper records and not the electronic records should be used to determine the result.
3. The use of internet, text message and telephone voting seriously compromises the security of an election, both because:
 - It is vulnerable to hackers and other attacks on the electoral system by those who might want to influence the outcome by interfering with the equipment or software;
 - Being a form of remote voting, it compromises the secrecy of the ballot, significantly increasing the risks of voter intimidation, bribery and impersonation.

The Society therefore opposes the introduction of internet, text and telephone voting at present.

4. The Society nevertheless notes the potential benefits of such forms of voting and the case for further small-scale experimentation. But unless it can be demonstrated that they are a necessary and effective way of increasing electoral participation, the Society opposes any wider use of these methods.