

# At Cross Purposes

**Prof. Simon Rogerson**

**Dr. N Ben Fairweather**

**Originally published as ETHicol in the IMIS Journal Volume 12  
No 3 (June 2002)**

The UK Government is pushing for all service delivery to be e-enabled by 2005, and as part of this process is looking at electronic voting. After all, a vote is, essentially, a piece of information, and the public are already used to voting by telephone and the Internet for television shows. Against this background, ministers such as Robin Cook have been keen to point out that voting by marking a cross in pencil on a piece of paper in a plywood polling booth seems to come from another era. The recent local elections in England and Wales have included several e-voting pilots as part of the Governments move to full implementation.

Electronic voting offers real advantages including the possibility of voting from more convenient locations and the chance for disabled voters to vote on equal terms with others.

However, voting is one activity where equal access is of vital importance: Robert Mugabe sought to influence the result of the Zimbabwe presidential election by making it easier to vote for those who he thought would vote for him, and more difficult for those he thought would vote against him. Unlike most public services, when it comes to voting, it is not good enough to make voting much easier for some people without making it easier for all. Voting systems cannot rely on a technology that some have easy access to, but a significant proportion is struggling to use. This alone seems to suggest that simply making it possible to vote using home computers will be unfair: less than about 40% of voters in the UK have access to PCs in the home.

E-voting also raises tough issues of security and secrecy. Virtually no other transaction with Government requires the same degree of secrecy, even from other family members. History has shown that if secrecy is not maintained, there will be attempts to buy votes, to coerce voters and to use undue influence in other ways. It is no good, therefore, if problems are encountered, to go back to receipts as in other electronic transactions: receipts are just what would be needed to buy and sell votes and make sure coercion has worked.

If voting is allowed away from supervised polling stations, how do we know that there is not someone else in the room coercing the voter? If we get to the stage where systems are routinely supplied with cameras, then it might be possible for there to be checks that

the voter is not being coerced, but this in turn will cause worries about privacy (see a previous ETHIcol edition on computer face recognition), and could be very labour intensive.

There is a clear requirement for the election authorities to know that each person who is submitting a vote is genuinely entitled to submit a vote, and has not already done so. Yet at the same time, the requirement for secrecy means that how the voter has voted should not be revealed to those in authority. This problem does not seem to be logically insoluble: issuing every voter in an election an identity code for that election, but which cannot be improperly linked back to the identity of the individual is part of the solution.

A fundamental problem for electronic voting or electronic counting of votes, is how do we know that we can trust the systems to give us a 'result' that accurately reflects how people have cast their votes. This is not just a case of how we avoid farces like Florida. The question of knowing whether we can trust systems goes deeper.

If you use ICT to cast a vote, how do you know that when you tell it 'vote for candidate X' it really does so? It might tell you that it has, but how do you know it is not telling lies? Part (but not all) of the problem here is with viruses. If you are using a multi-purpose computer with a mainstream operating system, you are wide open to virus attacks. Sure you might have 'virus protection', but virtually all 'virus protection' systems only protect you against viruses that they already know about, and there is no guarantee that it will know about a virus that changes votes as you cast them.

Assuming that all votes that are sent do genuinely reflect the intentions of the voters, how do we know they have been counted accurately? We could ask the computer to count them again, and be amazed when it comes to exactly the same result as last time (unless we are using the punch cards they used in Florida...). But that does not tell us that it has counted them correctly either time. Part of the solution here is for the software that does the counting to be open to inspection by the political parties (or experts they nominate), but that does not tell us that it has been compiled in the way that we expect. So the compiler needs to be open to inspection, and the computer that the compiler runs on, and so on, and so forth. Transparency is therefore key.

Even if we are confident the votes in the database are correctly counted we also need to know that they were recorded correctly in the first place, and the database has not been improperly modified. It is far from easy to ensure this in the face of people who might be determined to rig an election.

Although it is not perfect, marking your vote in pencil on a piece of paper in a plywood polling booth still has much to commend it. The challenge for those thinking about evoting is to come up with something that improves on that, but without throwing away the essential advantages that pencil and paper has. Politicians through to developers must work together in a socially responsible way to ensure electronic voting promotes the

democratic process. They must have the courage and conviction to reject the technological solution if this is not the case.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson  
Director  
Centre for Computing and Social Responsibility  
Faculty of Computing Sciences and Engineering  
De Montfort University  
The Gateway  
Leicester  
LE1 9BH  
Tel:(+44) 116 257 7475  
Fax:(+44) 116 207 8159  
Email:<srog@dmu.ac.uk>  
Home Page: ( <http://www.ccsr.cse.dmu.ac.uk> )