

ippr Seminar:
“E-voting: Policy and Practice”
Background Paper

Introduction

Voter turnout in the UK has been steadily falling, particularly in local and European election, while turnout for the General Election fell sharply from 71.5% in 1997 to 59.4% in 2001¹.

In response to this, as well as accusations of becoming increasingly remote and facing a trend of political disengagement from voters, the UK Government published a consultation paper *In the Service of Democracy*² which sought to identify how new technologies could increase public participation in democracy.

A major component of the proposals was the envisaging of a modern e-voting system which would encompass:

- Online electoral register;
- Online registration and online applications for postal votes;
- Online and text voting; and
- Electronic counting and collating of election results.

The paper outlined an action plan culminating in an e-enabled general election taking place sometime after 2006. As part of this process, 15 pilot schemes involving electronic voting or electronic counting took place during local elections in 2002, and over 160,000 citizens cast their votes by electronic means the following year.

Internationally, the use of e-voting has expanded dramatically. In the forthcoming US presidential election, over 50million voters will use electronic voting systems. This figure represents nearly 30% of registered voters. Only 1million (0.6% of registered voters) will use paper ballots³. In India's 2004 General Election, 390million people voted using one of the 700,000 electronic voting machines used at polling stations across India over a period of 3 weeks⁴.

Recently, such process of voting reform in the UK suffered a setback with criticisms from the Electoral Commission of all-postal voting pilots taking place in 2004⁵ and the likelihood that no pilots involving e-voting will take place in 2005⁶. In the main these criticisms have centred on security and logistical concerns regarding the safe production and collection of ballots. There are also significant costs involved in providing pilot schemes. However, the Greater London Authority has recently issued a tender notice for an e-voting system for use in the 2008 Mayoral and London Assembly elections.

¹ Electoral Commission (2001), *Election 2001: the Official Results*

² Office of Deputy Prime Minister (May 2002), *Implementing Electronic Voting in the UK*

³ Election Data Services (May 2004), *2004 Voting Equipment Table*

⁴ <http://www.indian-elections.com/facts-figures.html>

⁵ Electoral Commission (2004), *Delivering Democracy? The Future of Postal Voting*

⁶ KableNET.com (Sept 2004), *Retreat from e-voting*

Electronic Voting Pilots in the UK

As part of the Government's project, numerous pilots involving e-voting, postal voting and other forms of multi-channel voting have taken place. Two of the largest pilots were undertaken by Sheffield and Swindon in 2002 and 2003.

Swindon

In 2002 Swindon Borough Council carried out multi channel e-voting for the May local elections. The pilot scheme offered the opportunity to vote remotely by the Internet, telephone and by post, as well as via the traditional method of polling station. Over 15% of votes were cast electronically and the overall turnout increased by 3.5%.⁷

The Swindon pilot allowed early polling via mobile electronic voting kiosks in residential care facilities and two community centres; it distributed locally held, non-networked electronic registers in polling stations and employed e-counting technology to count paper ballots.

To use a kiosk, the voter applied for a vote and an electoral officer configured a ballot smart card using the electronic register. The smart card was then inserted into the kiosk unit by the electoral office. The voter can then select their chosen candidate and confirm their choice. The electoral officer then takes the smart card to be reprogrammed for a subsequent voter.

To prevent interference with the data, the electronic registers and kiosks were not connected to any network thus any attack would have to be a physical one on the unit itself. There was no electronic transfer of data at all: the kiosks were transferred physically to the count.

In 2003 the pilot was scaled up to include 7 day multi channel voting via the internet, telephone, interactive digital TV, and access information kiosks as well as standard postal and traditional ballot box voting.

The voting process was similar for each of the four e-voting channels. The voter first logged on by entering a 10 digit ballot code from their polling card, the system would then confirm the code was valid and had not already been used. If voting via the internet, digital tv or kiosk voting, the voter was presented with a list of candidates and could view a short statement from each.

The voter would then select their chosen candidate using either a two digit code if voting by telephone or by selecting a box using a mouse or touch screen for the other three channels. The system then confirmed the selection and gave the voter the opportunity to change their decision.

Finally the confirmed choice and the fact that the voter had voted were transmitted to a central computer and stored separately. After the polls had closed the e-voting results were sent by encrypted mail to the count centre where they were added to results from the ballot papers.

Sheffield

⁷ Electoral Commission (May 2003), *Pilot Scheme Evaluation – Swindon Borough Council Part A*

In 2002's May local elections residents of Sheffield were able to cast their votes over the Internet, via SMS or at the city's public information kiosks. In 2003 the pilot was scaled up to include touchtone telephone voting and an elector's smart card.

Electronic voting was available from 9am on Friday 25 April until 9pm on Thurs 1 May. To enable electors to vote using the pilots they were sent polling cards which provided the reader with a numeric 4 digit password hidden by a security foil, a 4 digit numeric receipt ID, a unique 2 digit voting code for each candidate to use in telephone and SMS channels. Posted separately were the 9 digit voter ID and personal smart card. As well as enabling electronic voting, the smart cards also provided access to a range of services including transport, libraries, leisure and payments.

In order to vote by the Internet, the voter was asked to log on to a specific website and follow onscreen instructions using their voter ID and password to authenticate themselves. Voters were given assurance of their vote through confirmation of their receipt ID as provided on the polling card.

To vote by SMS texting the voter was required to write a text message then send this to the number given for the relevant ward. The text message was coded thus:

'voter ID <space> password <space> ward code <space> unique voting code'

The voting code was provided on the polling card to identify the chosen candidate. Once the vote had been received, a confirmation message was sent to the voter which included the voter's personal receipt ID.

Using the telephone, the voter was asked to call a number on the reverse of the polling card. Once connected spoken instructions guided the voter through the process which including submitting voter ID and password to be authenticated, followed by the voting code for the chose candidate. The voter was then given their receipt ID as confirmation.

Sheffield also offered voting by public kiosk and provided touch screen kiosks which followed a similar process to internet voting. Voters could either authenticate themselves by submitting their voter ID and password or by using smart cards.

To prevent multiple voting, each ID and password was checked against an electronic register and once used could not be used again.

Evaluation

Both schemes found an overall improvement in turnout and, although turnout fell in Swindon from 31.2% in 2002⁸ to 29.9% in 2003⁹, both percentages were above the 2000 turnout figure. In Sheffield the net increase in turnout was 5.17%. In Swindon 61% of people surveyed said they felt e-voting measures made the process of voting better and 94% said they would use e-voting again in a General Election. In Sheffield 34% of voters and non-voters said the new arrangements either would have encouraged them or did encourage them to vote with telephone and SMS rating highest for both convenience and privacy¹⁰.

⁸ Electoral Commission (May 2002), *Pilot Scheme Evaluation – Swindon Borough Council Part A*

⁹ Electoral Commission (May 2003), *Pilot Scheme Evaluation – Swindon Borough Council Part A*

¹⁰ Electoral Commission (May 2003), *Pilot Scheme Evaluation – Sheffield City Council Part A*

However these improvements came at significant cost with non-technical and suppliers costs combining in Sheffield to give a minimum cost per e-vote of £55. In Swindon the total cost of the pilot was £ 589,648.

Although neither pilot scheme suffered verified cases of electoral fraud there were nonetheless concerns that contingencies had not been properly planned for, particularly in the Sheffield pilot where the unavailability of electronic registers for a brief period meant that people were turned away from poll stations.

Electoral costs and conveniences – the benefits of e-voting

In her paper, *E-voting as the Magic Ballot?*¹¹, Pippa Norris identifies three factors as contributing to the likelihood of a member of the electorate casting a vote: electoral costs, electoral choices and electoral decisiveness.

Electoral costs amount to inconveniences for the electorate. They may consist in registering to vote, if this process is long, arduous and indeed has to take place at all, sorting through information relating to the election and deciding how to vote and, finally, casting a ballot. Electoral choices are determined simply by the range of candidates or parties standing at the election. Electoral decisiveness translates as the extent to which votes cast for each party determine the outcome: a closely fought contest with no significant majority for any party is more likely to mobilise the electorate than a poll within an area of party stronghold.

The principal is that turnout will be affected accordingly as you increase or decrease each factor. Electronic distance voting i.e. at a time and place of the voter's choice certainly increases convenience. Swindon Council's online survey of internet voters found that 91.8% felt it was much more convenient to vote electronically relative to a polling station. It therefore contributes to a reduction in electoral costs.

However, the introduction of a simpler polling mechanism does not affect the other costs identified – registering, sorting through information – nor would it make any difference to the remaining two factors: choice and decisiveness. On this analysis it is easy to see why electronic voting is often labelled a “luxury” consideration existing on the margins of e-democracy.

One advantage of e-voting machines is the increased privacy they provide for disabled voters. In 2002, the US Congress passed the Help America Vote Act which required polling places to provide the same privacy and independence to all voters by 2006. The majority of e-voting machines now come with the ability to produce an audio recording of the ballot which can be listened to on headphones. The recorded instructions guide them on how to vote using the keyboard.

In addition for those who are not blind but have poor eyesight, text size can be increased and the height of machines can be altered for those in wheelchairs.

E-voting also has the potential to minimise the number of miscast votes. For example, machine settings can make it impossible to vote for two candidates, and many ask for confirmation of choice before the ballot is actually cast. However it is important that usability is central to the design of the electronic ballot. In one e-enabled election there were two many candidates to fit on one screen snapshot so the voter had to scroll down to view all of those standing. This could have an

¹¹ Pippa Norris (2002), *E-Voting as the Magic Ballot? The impact of the Internet on electoral participation and civic engagement*

adverse effect on candidates not immediately shown on the screen and cause them to lose votes.

Electronic counting systems can bring great benefits in terms of speeding up the counting process. In India the electronic system allowed the results to be announced a matter of hours after the polls closed; counting had previously taken two days. However results are not always accurate. In the November 2003 municipal election of Boone County, Indiana 140,000 votes were recorded in a county of 50,000 residents of which only 19,000 were eligible to vote¹². In this case, the machine had been programmed to give an excessively high count if a fault had occurred: an excessively high count which was picked up when only 5000 votes were actually cast. But the question remains whether this would be noticed in a larger state or county wide election.

The problem with many e-counting systems is that a re-count will merely constitute pressing a button and getting the same result. When coupled with an e-voting system that does not provide a paper audit trail and thus enable the independent verification of the result, there is no way to be certain of the veracity of the count.

Security

Identification

A major problem to overcome for remote e-voting is identification of the voter. Pilots in Swindon relied on pin codes and passwords mailed to the electorate. It is of course possible that such posted matter could be stolen from hallways of houses of multiple occupation, mislaid and lost, but this equally applies to traditional ballot cards. More worrying is the ability of computer hackers to crack the code which provides such passwords and pin codes. Since passwords have to be useable, they can't be too long. However this makes them vulnerable to attacks. Whereas with traditional ballot box voting, stealing votes would be a long and arduous process involving procuring perhaps several thousand ballot cards in order to have an impact on the result, electronic methods could enable the creation or theft of thousands of votes from one location.

Sheffield's election pilot included the distribution of an elector's smart card providing another means for proving identification without relying solely on passwords. However, smart cards are still vulnerable to fraudulent activity. In the first place there remain logistical issues around getting the right card to the right user and in the end, unless combined with pin codes to make them marginally more secure, they only authenticate the machine – anyone could have put the smart card in.

This has led some to argue that remote e-voting cannot be considered without the use of the 'basic infrastructure element'¹³ of ID cards. An identification card using biometrics (i.e. retina, finger or voice prints) can combine a digital identity with a 'real' identity as well as providing secure storage for an electronic ballot token for use in an election. The costs of creating and maintaining a biometrics database however, are huge, and to use them only in elections would be to create election costs way in excess of benefits remote e-voting may deliver. For an ID card scheme to be implemented in Britain, the Government has estimated a cost of £31bn. The solution is of course to use ID cards for access to a range of other public services. Aside

¹² Grant Gross (2003), 'Voting machine glitch shows thousands of extra votes', IDG News Service

¹³ Robert Kofler et al (2004), *The Role of Digital Signature Cards in Electronic Voting*, Proceedings of the 37th Hawaii International Conference on System Sciences

from the human rights debate surrounding implementation of ID cards, there is also a danger that a biometrics database could be compromised and thus, since new biometrics data could not be issued, the entire project rendered worthless.

Recording and transmitting

Security concerns common to the Internet are just as relevant to remote e-voting using a network. Such systems would be vulnerable to instances of hacking, just as other computer-based systems, such as Internet banking are. Firewalls can be deployed as protection however they are not foolproof and there will always remain the danger that a hacker may be able to manipulate data by altering or removing votes from the system.

Similarly, such a system would also face the familiar problem of viruses. Again, technological precautions such as anti-virus software can be put in place but neither can these be 100% guaranteed.

E-voting systems are provided by private companies with commercial interests to protect. To this extent, many are reluctant to release the source code behind the e-voting technology they deploy. There have been calls for such information to be made available to the public under 'open source' guidelines, most notably by the Chairman of the Election Assistance Commission in the US¹⁴. However, there are counter-claims that this would make such systems more vulnerable to attack from hackers.

A major security scare occurred recently with the discovery of source code used by Diebold¹⁵, who are supplying 75,000 electronic voting machines and tallying equipment across the US, on an FTP site the company had failed to properly secure. The Code was referred to Avi Rubin, a computer scientist at John Hopkins University, who then published a report¹⁶ in 2003 highlighting serious flaws including some basic errors that would leave the code vulnerable to external and internal manipulation.

This and the fact that some companies allow only 'authorised personnel', i.e. company staff, to inspect the machines has led to accusations of private companies relying on a 'trust us' mentality¹⁷. This is against principles of transparency that are required within an electoral system to allow public inspection and review prior to and after any election.

Attacks can also take place against the network. Denial of Service (DoS) attacks occur when "a deliberate attempt is made to stop a machine from performing its usual activities by having another computer create large amounts of specious traffic. The traffic may be valid requests made in an overwhelming volume or specially crafted protocol fragments that cause the serving machine to tie up significant resources to no useful purpose"¹⁸. It is estimated there are currently over 4000 attempted DoS attacks a week, and such attacks have in the past caused e-commerce services such as e-bay and Amazon to be inaccessible for short periods of time. As elections are time critical, the potential for disenfranchising voters is huge. It is also likely to be difficult to assess whether a DoS attack is happening, as

¹⁴ Declan McCullagh (2004), '*E-voting to go open source?*', Silicon.com

¹⁵ www.diebold.com

¹⁶ Avi Rubin et al (2003), '*Analysis of an Electronic Voting System*', Johns Hopkins University Information Security Institute Technical Report TR-2003-19

¹⁷ Rebecca Mercuri (2004), '*A Better Ballot Box?*', IEEE Spectrum Online

¹⁸ All Party Internet Group (2004), "*Revision of the Computer Misuse Act*"

it may take the form of legitimate requests and in a large scale election, this would be difficult to distinguish from actual voting activity.

The dangers posed by corruption of electronic data, either by intended attack or technology based network or system failure again adds weight to the argument for paper audit trails.

Rebecca Mercuri, an e-voting sceptic, has pushed for the provision of a “voter-verified physical audit trail” which can be used to authenticate election results and provide the transparency many current electronic voting systems lack.

The ‘Mercuri Method’¹⁹ includes as a process the printing of a paper ballot containing the selections made on an electronic voting screen. The ballot is displayed to the voter behind a glass screen and can be inspected for mistakes. If correct, it is deposited mechanically into the ballot box. If the voter identifies a mistake, an election official can be informed and the ballot voided.

The advantages of this method are that, while enabling a quick preliminary count by electronic tally, a paper recount is possible. It also demands secondary verification from the voter themselves and is thus likely to reduce instances of over or under voting. However, this system is not compatible with remote voting: the voter must be physically present at the polling station in order to cast their vote.

Privacy

One of the fundamental principles of elections is that each voter should have the right to vote in privacy with there being no means of outside influence or coercion, nor any way to match voter to vote cast.

Remote electronic voting faces the same possible criticisms levelled at postal voting: when the casting of a ballot takes place away from the traditional polling booth, it is possible for individuals to be pressured into voting for a specific candidate and for the coercer to demand proof in the form of the completed ballot. This would not be possible using traditional poll booths where only one person is allowed to access the booth at any one time.

There is little solution to offer here, although it should be recognised such methods of exerting pressure on individuals would struggle to impact on a large scale election. Offering multi-channel voting methods, including poll booths, would allow those who feel themselves at risk from such pressures to continue to vote in a completely private environment.

Conclusion – what next for the UK?

Despite criticisms from the Electoral Society of all-postal voting schemes, and continuing concerns surrounding security and privacy, the UK Government remain committed to an e-enabled General Election post 2006. In *Implementing Electronic Voting in the UK*, the Office of the Deputy Prime Minister state there should not be a large scale national implementation of remote electronic voting until issues of secrecy, security and technological penetration have been addressed.

¹⁹ Rebecca Mercuri (1992), ‘Physical Verifiability of Computer Systems’, 5th International Computer Virus and Security Conference

As of March 2004, 53% of UK households have digital television and 53% of UK adults have internet access at home. While 96% of the UK's population are aware of a place where they can readily access the internet, be it at home, work, using mobile technology or a public access point, Internet usage still roughly follows patterns of socio-economic divide²⁰. Public access points were also rated highest in terms of security and privacy concerns in Swindon's voter survey following the 2003 pilots. The telephone remains the tool nearest to providing universal access, however pin codes traditionally used in telephone voting are subject to attack as highlighted above. It is imperative that the Government maintain multi-channel voting, not only for the purpose of providing alternatives in case of single system failure, but also to ensure access to voting for all sectors of society.

The benefits of Identity Cards in terms of providing remote identity authentication are clear. However there remain numerous logistical and philosophical issues surrounding their introduction. The financial cost of developing a biometrics database would be inproportionate to the benefits of convenience and increased security it would bring to the voting system. Meanwhile, the human rights cost of using Identity Cards for more than just e-voting are a frequent source of debate.

While it may be the case that identity cards are a 'basic infrastructure element' of e-voting, this should not be used as an argument for or against their implementation. As noted above, practical costs of an Identity Card system force the issue out of the realm of e-voting and into more complicated debates concerning levels of Government surveillance and human rights.

The pilot studies referenced in this paper suffered no proven cases of fraud. While there were problems with availability of electronic registers in Sheffield for a brief time, the pilots on the whole were conducted smoothly and received high levels of voter satisfaction. But there remains the possibility of fraud, manipulation and system failure. The Government has previously given a commitment that it will only introduce remote voting on a national scale once these issues have been resolved. The relative success of the pilots should not be taken as evidence that e-voting is now secure. A much larger and higher profile case study of e-voting and e-counting will soon be available in the form of the US General Election. With the global media attention focussed on 2nd November, as well as numerous e-voting security scare stories, the stakes are significantly higher and security and systems are more likely to be tested both by malicious external interference and internal system failure.

In *Implementing e-voting in the UK*, the Government recognised that new technologies "can be used more extensively as a tool for public policy making". It is recommended the Government consider the potential of new technologies for increasing public participation in this context, rather than focussing on e-voting to bring about an increase in voter turnout. Further study into how new technologies can facilitate public debate and interaction with local and national Government should be undertaken and any recommendations given priority in the public participation agenda.

²⁰ Cabinet Office (2004), *Enabling a Digitally United Kingdom*, Report of the Digital Inclusion Panel

ERROR: undefined
OFFENDING COMMAND: ,JrrAB31bTk26S,98\$,,U6S*I

STACK: