OPEN RIGHTS GROUP

Electronic Voting

A challenge to democracy?

January 2007

Prepared by:
Jason Kitcat, E-voting Co-ordinator, Open Rights Group

For more information, contact:
+44 (0)20 7096 1079
12 Duke's Road, London WC1H 9AD
michael@openrightsgroup.org
www.openrightsgroup.org

About the Open Rights Group

The Open Rights Group is a fast-growing NGO focused on raising awareness of issues such as privacy, identity, data protection, access to knowledge and copyright reform. Founded in 2005 by a pledge from 1000 members, ORG is funded by small grants and donations from supporters. We aim to improve both understanding and policy in digital rights matters that affect both businesses and the public. Our activities include organising campaigns, lobbying government, and helping journalists find experts and alternative voices for stories.

The Open Rights Group's goals are to raise awareness of digital rights abuses; to provide a media clearinghouse, connecting journalists with experts and activists; to preserve and extend traditional civil liberties in the digital world; to collaborate with other digital rights and related organisations; and to nurture a community of campaigning volunteers, from grassroots activists to technical and legal experts.

The UK is to hold more electronic voting pilots during the May 2007 elections, despite serious problems with e-voting technology.

Contrary to the global trend away from electronic voting, the British government has announced — after a three year hiatus — a new series of electoral modernisation pilots which include e-voting and electronic vote counting.

Countries worldwide are learning that expensive e-voting technologies are not as secure, accurate or reliable as suppliers promise. Systems fail on election day, software bugs prevent votes being recorded, voters find the interfaces hard to use, and recounts turn out to be impossible. These problems occur even when authorities have implemented testing, certification and audit processes for the systems being used.

Lessons could have been learnt from the e-voting pilots that have been held in the UK since 2000 and the experiences of other countries, but they have not. Instead, the Government has plunged headlong into a new round of e-voting pilots without any audit, testing and certification processes, or meaningful oversight by technically competent bodies. They have ignored calls from both vendors and the Electoral Commission to allow more time for implementation, so 2007 will see another rush to be ready by election day.

Why is e-voting being foisted onto our democratic process? In the white papers *Modern Local Government* (1998)[1] and *Modernising Government* (1999)[2] the Government says that elections must be modernised. Ministers believe it will improve engagement: the 2007 pilot prospectus by the Department for Constitutional Affairs argues that e-voting could stem declining turnout, in spite of evidence to the contrary. In fact, turnout fell during the 2003 pilots[3].

Still, even if turnout isn't improved by e-voting, why worry? How disastrous can the modernisation of elections be? We trust our banking, our hospitals, and even airplanes to computers — how could this be any different?

Voting is a uniquely difficult question for computer science: the system must verify your eligability to vote; know whether you have already voted; and allow for audits and recounts. Yet it must always preserve your anonymity[4] and privacy. Currently, there are no practical solutions to this highly complex problem and existing systems are unacceptibly flawed.

E-voting threatens the integrity of our elections and we oppose its use in our democracy.

A point of clarification: e-voting is not e-democracy

It is important to understand that e-voting is not the same as e-democracy: they are distinctly different technological fields. The Open Rights Group supports developments in e-democracy, such as using the web to facilitate public consultations or improve people's access to their local, national and European representatives. But voting is a very particular case which, for the reasons explained below, is not best served by introducing new technology.

The secret ballot is essential to democracy

Voting is the fundamental action of democracy. By casting a vote we hold previous politicians to account, choose new representatives, and take a stand on issues important to us. Of course democracy is more than votes – it's debate, letter writing, campaigning and consultation – but the vote is how every single citizen can wield real and immediate power. It's incredibly important that everyone can vote without interference, safe in the knowledge that their vote will be counted.

Through the long history of democracy we have learnt that in the pursuit of power some groups are willing to threaten voters to make sure they vote 'the right way'. But if the vote is secret then there is no way for intimidators to know whether someone has voted for them or not and so threats become useless. The secret ballot is an important, fundamental right that protects voters and the integrity of our elections.

Votes are a vital expression of the people's power which must be both secret and restricted to only one per citizen.

Pencil and paper protect us from electoral fraud

Voting began 2,500 years ago in Athens, but it wasn't until the 17th century that paper ballots began to re-emerge for use in political elections. These paper-based elections wouldn't have met modern standards. Ballot papers were provided by candidates or voters, so they could be pre-printed with all the votes marked for one party. They could also be different colours, shapes and sizes, so it was easy to know how anyone had voted, just as if they had called it out in public.

It took a series of innovations in the Australian colonies from 1856 onwards to create the Secret Australian Ballot. For the first time the ballot was printed by officials, delivered to the voter who marked it with a cross next to the preferred candidate and deposited in the ballot box under government supervision. The Australian method was rapidly adopted around the world from the 1870s

onwards in response to rampant electoral fraud: vote buying, intimidation, bribery, bullying, threats from employers and dizzying amounts of money spent by candidates on alcohol for voters.

In the UK, pressure to introduce the secret paper ballot surfaced around 1819. The number of people winning the right to vote grew dramatically throughout the 19th century, yet voting was still done orally to a returning officer and a clerk. Despite widespread fraud, King William IV and many 'English Gentlemen' opposed the secret ballot. It took a gruelling 50 year campaign and examples from around the world, including Australia, to persuade Parliament, finally, to pass the 1872 Ballot Act. This was set to expire in 1880 but the Secret Australian Ballot's positive impact was indisputable and, in 1882, the Ballot Act's changes were made permanent.

Since then, to further combat fraud and intimidation, improvements have been made to voter registration and the security of the ballot. These have been incremental improvements on a proven system that has evolved in the face of corrosive and brutal electoral fraud. This is a system that protects itself, as well as the voters.

Why is e-voting a difficult problem?

First, let's consider the international standards an election has to meet to be considered free and fair:

- Individuals have to be accurately identified as eligible voters who have not already voted.
- Voters are only allowed one anonymous ballot each, which they can mark in privacy.
- The ballot box is secure, observed and, during the election, only able to have votes added to it by voters. Votes cannot be removed.
- When the election ends the ballot box is opened and counted in the presence of observers from all competing parties. The counting process cannot reveal how individual voters cast their ballots.
- If results are in doubt the ballots can be checked and counted again by different people.

We can formulate three basic steps for a computerised voting system: check that a user is entitled to vote and hasn't already; show the user the ballot and record their vote; and, finally, count the votes.

At first glance this appears to be just like selling goods online: check that a user is who they say they are so that they can use the credit card on record; show the items they can buy; then process the order and send out the goods.

But these similarities are only superficial. When you shop online the merchant knows who you are at all times, otherwise they wouldn't be able to charge your card or know where to send your purchases to. But in an election we cannot associate your identity with your vote without breaching your privacy, yet somehow we need to be certain that you actually are entitled to vote. To prevent ballot stuffing, we must mark your vote so that we can be sure it came from a real voter, yet we cannot trace this vote to you personally.

It turns out that this is an extremely difficult cryptographic problem that still challenges top scientists and there simply are no solutions which are practical and which fulfil all necessary criteria.

In the meantime e-voting suppliers are selling systems they believe are 'good enough', but which make compromises. The problems with e-voting arise not only because these compromises are made, but also because of the difficulties of building any large-scale computer system.

All election counts have some problems due to human error. However these errors are random, as likely to affect one candidate as another, so that overall the result is fair. If errors become systematic, such as if an e-voting system doesn't register any votes for one candidate, or counts backwards for one candidate whilst counting forward for another, then the errors aren't evenly distributed[5]. This means that one candidate is more likely to be affected than others and so the election result isn't a fair representation of voters' intentions.

These types of errors can have serious implications: small vote manipulations of less than 1% in key marginal seats can swing the results of elections in first-past-the-post systems such as that used in the UK[6]. And, as will be shown below, countries with voting systems less sensitive to fraud than first-past-the-post are already withdrawing e-voting systems.

Common forms of e-voting

Kiosk

Kiosk e-voting consists of dedicated machines being used in the polling station or elsewhere, such as shopping malls, to let electors cast their votes. Votes are cast using buttons or a touch screen and are stored in an electronic memory. If used in a polling place, kiosk systems have the advantage of being supervised.

But unless a paper ballot is printed at the time of voting and checked by the voter, manual recounts are not possible. If there are any technical problems or attempts at fraud, polling station staff lack the skills to resolve matters; they are dependent on support from the e-voting supplier. This support is

often sub-contracted, but regardless it is inevitable that voters will be forced to wait until support staff can atttend the polling station. In America, this has resulted in a need for court injunctions to decide whether the polling station can stay open long enough to let waiting voters excercise their right to vote.

Kiosk machines are costly, particularly in light of the fact that they can only be used for elections. Whilst kiosk machines can provide audio and other input/output features to help voters with disabilities vote alone, they are only shifting their trust from a helper in the polling station to a system they cannot be sure is voting as they desire.

Remote (Internet)
Voters sit at home or in a library and use a computer, digital television or mobile phone[7] to mark their ballot.

Elections held using remote voting can be contentious because it is difficult to verify that the voter is who they claim to be. Both anonymity and privacy are compromised because others can watch the elector vote. This opens the door to voter coercion and vote buying.

There are technical problems too. The system is vulnerable to attacks both on the central e-voting server and on each computer used to vote. These attacks may disrupt the process of voting or bring the results into question. Meaningful recounts are not possible as all the authorities have is a database of votes, with no paper trail for audit.

Renowned cryptographer and computer security expert Bruce Schneier argues that “a secure internet voting system is theoretically possible, but it would be the first secure networked application ever created in the history of computers.”[8]

Phone
Votes are cast either through a touch-tone system (similar to that used for television votes) or through SMS text messages on mobile phones. Authentication is achieved through the use of PIN and access codes that are mailed to voters ahead of the ballot.

While proven in entertainment settings where there are no requirements for authentication, such systems are not suitable for democratic elections. Phone voting depends on highly centralised, private infrastructures which, in the case of SMS, are also unreliable and insecure (SMS messages are sent ‘in the clear’ and so could be intercepted). Thus privacy is virtually impossible

to maintain and security is based more on commercial confidentiality and control of the connections than any explicit protocols (such as SSL on the web).

Indeed TV production companies encourage multiple-voting as a way to increase their revenue from each vote cast. For the very enthusiastic fan, software is available on the internet which automates dialing, allowing a single individual to vote hundreds of times.

e-Counting

Specially designed ballots are marked by voters in such a way that an optical counting machine, i.e. a computer, can read them. The advantages of the paper ballot system are retained, but counts are quicker and if problems arise recounts of the ballot can still be done by hand.

However, computer-readable ballot papers can be confusing for some voters, resulting in errors and lost votes. E-counting systems are as vulnerable to fraud and error as other forms of e-voting technology, and unless the ballot papers are regularly audited and counted, then incorrect or fraudulent results can escape detection.

e-Voting tales of woe from around the world

Electronic voting has been introduced in many countries worldwide, only for serious doubts to be raised about the security, accuracy, reliability and verifiability of electronic elections.

Italy has announced its intention to no longer pilot e-voting methods. Making the announcement, Italian Minister of the Interior Guiulano Amato said that "We decided to stop the electronic voting machine … It will be the triumph of our ancestors … Let's stick to voting and counting physically because [it is] less easy to falsify."[9]

Security researchers in The Netherlands have discovered serious flaws in a model of e-voting machine widely used by the Dutch government and purchased by the Irish. The flaws, which included being able to remotely detect how a vote was cast from the machine's radio emissions, were confirmed by the Dutch Intelligence and Security Service. Subsequently a government review led to the withdrawal from elections of e-voting machines from a competing supplier.[10]

The Republic of Ireland has a moratorium on its e-voting machines after an Independent Commission, created after repeated cross-party criticism,

uncovered serious technical and procedural flaws. One telling finding from the Commission's second report was that "the testing of the [e-voting] system as a whole carried out to date, as well as the investigation, analysis and independent testing and certification of its individual components, [was] insufficient to provide a secure basis for the use of the system at elections in Ireland."[11] According to Freedom of Information releases, Ireland spent €110.4 million on e-voting between 2002 and May 2004.[12]

The Canadian province of Quebec has an indefinite moratorium on the use of its e-voting machines following the investigation of troubled municipal elections. Delivering his report on e-voting, Quebec's Chief Electoral Officer said that e-voting systems "[do] not offer sufficient guarantees of transparency and security to ensure the integrity of the vote."[13]

The United States, which has been a pioneer in using technology for elections, has a long history of problems with e-voting, some of which raise doubts as to the legitimacy of results. In 2004, a group of experts issued a report critical of a planned internet voting system for US soldiers overseas, resulting in the project being cancelled. They wrote that "the vulnerabilities … cannot be fixed by design changes or bug fixes to [the system]. These vulnerabilities are fundamental in the architecture of the internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough."[14]

In November 2006, America's influential National Institute of Standards & Technology stated that electronic voting machines "in practical terms cannot be made secure."[15] This is a view shared in prominent journals by leading computer science and elections academics around the world.

Doubts over the veracity of election results in the United States — including the 2000 Presidential count in Florida, the 2004 Presidential count in Ohio and the 2006 mid-term elections —have all revolved around failings or manipulations of e-voting systems. By January 2007 one Congressional seat was still in limbo due to 18,000 questionable votes cast with an e-voting system[16]. The flimsy e-voting certification process in the US has also been called into question after one of the key testing labs was secretly suspended in 2006[17].

These international experiences have shown that when electronic and software technologies are introduced into the election process, significant and worrying problems arise.

e-Voting is a black box system

Voting technology is what is known as a 'black box': voters, candidates and even officials cannot see the inner the workings of the machines. Only a small group of technology experts has any hope of understanding how the election is being conducted and counted. Because the votes are invisible, made up of ones and zeroes, it is extremely difficult even for experts to be certain that what vendors claim is happening really is happening.

Manipulating bits in a computer is much easier than copying paper ballots, so there is potential for undetectable vote manipulation on a scale never seen before: a hacker could hide a tiny piece of code in the voting software that could invisibly, but significantly, modify an election's results. But putting aside undetectable hackers, vote stealing and other manipulations, we must also remember that these systems are built by ordinary, fallible people.

Like all computers, e-voting systems go wrong and usually do so on election day because this is the only time they are used. And the problems that come to light are not trivial. There have been cases where selecting one candidate stored a vote for another, or where the system failed completely, depriving people of their right to vote. Problems are often not discovered until the election is over, when it is impossible to say how the votes should have been cast.

Because the votes are stored as bits, there is nothing for election officials to study when problems occur, as there is with paper ballots. There is nothing to audit except some memory cards, which cannot shed any light upon what happened but can only provide a final tally. There is no way for the voter, candidates or officials to know whether the voter's intent was accurately stored and then correctly counted by the e-voting system. Everything happens inside the black box.

With a paper ballot the voter can see their mark and has immediate feedback. That mark is stored, unchangeable, in the ballot box until it is time to be counted. If a recount is required, that ballot can be examined a second time.

It would be trivial for an e-voting system to report that it has stored a vote for Ms X when in fact Mr Y gains one vote in the memory card. Under these circumstances, a recount is no help, as the computer adds the same numbers up again and will arrive at the same result each time. With paper, new people can be called in to count and judges can debate each ballot paper, but with e-voting the election is nothing but the numbers on the screen.

These fears are not just theoretical. Activists in the United States worked with a Finnish computer security expert and a respected election official in Florida

- to show how manipulation of a memory card before an election started would allow results counted by an optical vote scanner to be altered without trace. The successful manipulation is shown as the conclusion of *Hacking Democracy*, a film documenting the many problems with e-voting based elections in the United States[18].

The vendors' love of secrecy

These risks are exacerbated by e-voting suppliers' insistence on commercial confidentiality, withholding access to the design and source code of their electronic voting systems. It is well known within the computer security field that the most secure systems are ones that remain secure even when their details are publicly known.

Developing e-voting software in secret leads to a situation where the system seems secure to the vendor, but is in fact vulnerable to attack. Indeed, every time security researchers have found ways to comprehensively test commercially available e-voting systems, they have revealed extremely serious security flaws[19]. Yet vendors and governments, including the UK government, maintain secrecy – which does not serve the integrity of our elections.

Paper trails: the imperfect voter verified audit trail

In the United States, where e-voting technology is already widely in use, experts and activists had a difficult task. It was not realistic for them to expect local authorities to ditch expensive e-voting systems in time for fast approaching elections; that would need to be a campaign taking years. In the meantime the best they could propose was advocating the introduction of 'Voter Verified Audit Trails'.

In practical terms this means that when an elector went to cast their vote electronically, their vote would also be recorded on a paper printout. The elector would inspect the printout to ensure it was correct and then confirm their vote. Thus if there were any doubts over the integrity of the e-voting systems, the paper ballot, which had been checked by the voter, could be counted in place of the electronic votes. It was a clever idea that would help maintain trust and accuracy in US elections and so it became widely adopted.

This was, however, a short-term fix and now activists are working hard with state and federal authorities to bring about deep reform of their electoral system. The paper trails are not perfect: printers can jam and voters are often confused by them. Additionally, if the paper printouts are never counted and compared to the tallies produced by the machines, there's never any check on the accuracy of the result presented by e-voting systems.

Given that the UK already has a strong polling station-based paper ballot electoral system, it is perverse to go to great expense installing complex computer systems with printers attached to them.

Remote voting opens the path for fraud

Apart from e-voting, the UK government has also been keen to push for postal voting under the same banner of boosting turnout. Pilots were run in numerous local and regional elections resulting in considerable publicity, mostly negative due to the problems experienced. Six councillors were found guilty of electoral fraud in Birmingham and one was found guilty of vote rigging in Blackburn.

Presiding over the Birmingham case, Judge Richard Mawrey said that "the [electoral] system is wide open to fraud and any would-be political fraudster knows that." He added that "anybody who has sat through the case I have just tried and listened to evidence of electoral fraud that would disgrace a banana republic would find [the Government's insistence that the current postal voting system is working] surprising."[20]

In response to this judgement, cross-party criticism and concerns from the Electoral Commission, new electoral administration legislation was passed in 2006 that addresses some of these concerns. Nevertheless postal voting's remote nature opens the way for voter intimidation and manipulation. Politicians in all parties continue to express concerns and the Council of Europe has launched an investigation into the UK's postal voting practices[21].

The Committee on Standards in Public Life recently commented: "Evidence to our inquiry demonstrated that the Commission should have shown greater focus and courage in alerting the risk to the integrity of the electoral process from legislative changes, principally the lack of safeguards against electoral fraud with the introduction of postal voting on demand."[22]

Postal voting is still paper-based, so the scale of the fraud possible is limited by the logistics of collecting and moving the ballot papers. It was this problem that lead to the Birmingham councillors being caught. With e-voting the paper is gone, hence the scale of possible fraud becomes as large as the fraudster's imagination.

Furthermore, software fraud can be committed long before an election, by someone far beyond the UK's legal jurisdiction, thereby making detection and prosecution difficult.

UK e-voting, past and present

May 2003 saw the largest electoral pilots ever, covering 14% of the English electorate, funded with £18.5m from central government, in addition to the usual local government electoral budgets. Mistakes were made, many of which were clearly identified in the Electoral Commission's evaluation reports[23]. In particular, the selection and management of e-voting vendors was heavily criticised.

Competing vendors were forced to work together without prior notice or contracts. Vendors took control of running elections from Returning Officers. There were no clear structures or lines of responsibilities in which vendors were supposed to operate. Local government staff were under-trained and counts were impossible to scrutinise as nobody except the vendors knew what was supposed to be happening.

Extremely tight implementation timescales imposed by the Government were roundly criticised by the Electoral Commission and vendors. The lack of time prevented proper testing and evaluation of the systems before elections. The little testing that was done was felt not to have been sufficiently independent of the suppliers. The Government's extraordinary view was that short timescales were inevitable and that vendors would get used to it.

Again in 2007 the timescale is extremely tight, yet by January 2007 the Government was already a month behind in a timetable that only allowed two months for implementation and testing. In 2003 the lack of time prevented proper security testing and analysis, complete risk assessment and usability testing. Are these absolutely necessary steps to be skipped again due to the lack of time?

None of the Department for Constitutional Affairs, local government or the Electoral Commission has the technical expertise to evaluate and manage e-voting vendors properly. The result is that vendors have to be trusted to run elections in a secure, reliable and private manner without proper external, independent testing and evaluation. This amounts to the effective privatisation of our election systems, as for-profit corporations, usually foreign-owned, are paid to completely administer our elections from start to end. We do not believe this is healthy for democracy. It is vital that elections are publicly-run and scrutinised.

Undoubtedly e-voting systems bring new risks, challenges and costs to our electoral process. So what are the benefits? Initially, claims were made that e-voting could save money spent in the electoral process. This was quickly discarded in favour of arguing that e-voting could boost turnout, particularly

with younger voters more accustomed to computers. However the evidence is that, given the publicity surrounding the novelty of e-voting, there is a negligible impact on turnout.

People usually choose to vote or not to vote for reasons other than convenience[24]. How close an election is, the proportionality of the voting system and media coverage all play a larger part in someone's decision whether to vote than convenience[25]. The Government's simplistic thinking that people vote electronically for *Big Brother*, *Strictly Come Dancing* or *X Factor* and so would like to do so for political elections isn't supported by the theory or turnout statistics.

The final claim that the Government makes is that e-voting will allow results to be returned more quickly. In a purely electronic election this is undoubtedly true but in the multi-channel elections that the UK government advocates paper and postal ballots still need to be counted.

So not only are the results untrustworthy, but is there little to be gained.

In 2003 Stratford on Avon District Council reported that votes had cost around £120 per internet vote and £22 per kiosk vote. Sheffield reported a cost of about £55 per electronic vote cast. Stratford stated that for ordinary elections their costs were less than £1 per vote cast. Can e-voting be worth such extraordinary costs and risks?

Conclusion

Electronic voting is an incredibly complex and very expensive technology that introduces new risks, doubts, and opportunities for fraud and failure. The benefits to the electorate are marginal, at best.

As recent postal vote prosecutions have shown[26], the UK is not immune to electoral fraud. Our electoral system has carefully evolved over centuries to protect the individual voter and the integrity of the results so that the will of the people is accurately expressed. This is an issue that affects all citizens and candidates from all parties: any side could be affected by systematic error or fraud.

Encouraging citizen engagement in our democratic system is an important and noble goal. However pilots have shown that e-voting is not an effective way to boost democratic participation. There is no reasonable argument for the Government to continue to pursue e-voting at great cost and great risk to the integrity of and trust in our electoral system.

E-voting threatens the integrity of our elections and we oppose its use in our democracy.

Endnotes

1 *Modern Local Government*, 1998, http://www.communities.gov.uk/embedded_object.asp?id=1165214

2 *Modernising Government*, 1999, http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm

3 There is some doubt about how far the turnout fell during the 2003 pilots, The Electoral Commission's main pilot evaluation report appears to have under-reported the fall in turnout. See: http://www.jasonkitcat.com/?be_id=323

4 Due to a historical anomaly brought over from an early version of the Australian Ballot, the British vote is not completely anonymous. A number on the ballot paper is noted against the voter's registration number in a version of the electoral roll. The ballots and voter identity can only legally be brought together if an investigation is ordered by a judge. This anomaly breaches the Human Rights Act and our treaty commitments to the UN and Council of Europe. For more information, see this government-sponsored legal analysis, *Implementing Electronic Voting*, Bob Watt, March 2002: http://www.dca.gov.uk/elections/e-voting/pdf/legal-report.pdf

5 For more on this issue see Bruce Schneier: http://www.wired.com/news/columns/0,72124-0.html

6 Di Franco, A., Petro, A., Shear, E. & Vladimirov, V. (2004). Small vote manipulations can swing elections. *Communications of the ACM*, 47(10), pp.43—45.

7 The DCA has excluded mobile phone and interactive TV voting from the 2007 pilots, but not ruled it out in the future.

8 Source: http://www.schneier.com/crypto-gram-0012.html#1

9 See: http://www.jasonkitcat.com/?be_id=320

10 See: http://www.wijvertrouwenstemcomputersniet.nl/English

11 Source: http://www.cev.ie/htm/press/press040706.htm

12 Source: http://fiasco.ie/evoting/resources/CostofElectronicvotingAsOfMay.pdf

13 Source: http://www.electionsquebec.qc.ca/en/nouvelleDetail.asp?id=2153&typeN=2

14 Source: http://servesecurityreport.org/paper.pdf

15 Source: http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf

16 House Seat Hangs by a Byte, Kim Zetter, *Wired News* (11 Jan 2007)
http://www.wired.com/news/technology/0,72452-0.html

17 Source: http://www.nytimes.com/2007/01/04/washington/04voting.html

18 *Hacking Democracy*, http://www.hbo.com/docs/programs/hackingdemocracy/

19 For example studies see: http://avirubin.com/vote/analysis/index.html
http://itpolicy.princeton.edu/voting/
http://www.wijvertrouwenstemcomputersniet.nl/English

20 Source: http://news.bbc.co.uk/1/hi/uk/4410743.stm More on the postal vote problems at http://www.jasonkitcat.com/?be_id=195

21 For more see: http://www.jasonkitcat.com/?be_id=292

22 For analysis of the Electoral Commission's criticisms and the Government's responses regarding the 2003 pilots see: *The Uncertain Nature of Elections to Come*: http://www.jasonkitcat.com/files/uncertain_elections.pdf

23 *Review of The Electoral Commission* press notice, Committee on Standards in Public Life, 18 Jan 2007. Source: http://www.public-standards.gov.uk/upload/assets/www.public_standards.gov.uk/pn202final.doc

24 For more explanation of the turnout issue, see: http://www.jasonkitcat.com/?be_id=317

25 Source: http://www.jasonkitcat.com/h/n/WRITING/edemocracy/ALL/43/

26 For summaries of the prosecutions, see: http://www.jasonkitcat.com/?be_id=195