

The uncertain nature of elections to come

Response and analysis to the Electoral Commission's
evaluation of the 2003 electoral pilot schemes and the
Government's own response to the evaluation

Jason Kitcat

founder & co-ordinator

the free e-democracy project

October 2003

Introduction

May 2003 saw the largest ever set of electoral pilots covering 14% of the English electorate funded with £18.5m of central government funds, a major boost over the anticipated £10m spend for the year (6.121)¹. As is to be expected some pilots went more smoothly than others. The Project submitted a report on problems experienced by Brighton & Hove's all postal pilot and numerous other reports highlighted troubles and glitches amongst many other pilots, particularly those testing electronic voting methods.

As a result many observers were keen to see how the Electoral Commission would report and comment on the problems encountered by the pilots. All participants and observers were even more eager to see how the Government would respond to the Commission's evaluation. These pilots not only mark a whole new scale of experimentation in voting procedures but the procurement process used has put in place the contractors and frameworks for the pilots until 2005. With a firm Government commitment to a multi-channel election after 2006 the 2003 pilots and their aftermath are vital to the future of elections in Britain.

This paper aims to examine the Electoral Commission's evaluation "The shape of elections to come: A strategic evaluation of the 2003 pilot schemes" and "The Government's Response to the Electoral Commission's Report" presented by the Office of the Deputy Prime Minister. Naturally press coverage was relatively cursory and relied on the executive summaries so this paper will highlight the overlooked technical and procedural issues that will truly impact the legitimacy and trustworthiness of any future electronic vote.

In the next section the key points regarding electronic voting from the Commission's evaluation will be discussed along with the Government's responses, where appropriate. The paper will then conclude with recommendations and thoughts on the future of e-voting in Britain.

¹ Note that throughout the Commission's report is referenced to by paragraph number e.g. (6.9) and the Government's response by page number e.g. (pp9)

Analysis

Contracts, Suppliers and Leadership

The Commission's report highlighted the confusing nature of the credentials (PINs, passwords etc) used in the pilots (6.8.-6.9). Not only did suppliers, in some cases, use different terminology than councils but different credentials were needed for each voting channel. The result was unnecessary confusion which may have threatened citizens' right to vote by their failing to recognise the vital importance of the credentials and how they could be used.

That such simple errors and confusion occurred should not be surprising considering the Commission's indictment of the pilot procurement process (6.19-6.21): Fundamental requirements, while improved compared to the muddle of 2002, were often unclear and some failed to specify the level at which they should be met. Indeed the Commission highlighted numerous areas where security requirements could be have been improved arguing that the Government left considerable ambiguity resulting in significant areas where security could have been improved (6.43). Due to the procurement framework used there was no single lead contractor with "end-to-end responsibility for delivering the solution" (6.23) resulting in a lack of clarity, particularly if disputes occurred. The report continues stating that "there were no clear service level agreements between the suppliers" and indeed sometimes competing firms were supposed to work together with minimal notice and no contracts. The Project regards such findings a serious indictment on the Government's approach to the pilots and its handling of the suppliers in particular. Instead of trusting the suppliers to muddle through as best they could the Government should be ensuring a strict and clear structure is in place for suppliers to ensure the smooth and secure running of the elections in question.

Despite the Commission questioning how much control and understanding Returning Officers had over the pilots and their suppliers the Government responded to these criticisms by championing the Officers' leadership role in these and future pilots (pp16). This view must be questioned as the Commission noted

The uncertain nature of elections to come

that in 2003 suppliers often took roles previously fulfilled by Returning Officers (6.29). It was further noted that staff frequently lacked training and guidance which particularly effected to scrutiny of counts. During counts for pilot elections data was often transferred manually (such as by email) and then imported into applications such as Word or Excel to collate results. Probably as a result several pilots encountered problems integrating counts from the various channels (6.35-6.36) and lacked publicly documented procedures for candidates or their agents to assess that proper actions had indeed been undertaken (6.62). In the Project's view all aspects of a vote should be strictly monitored and controlled, to have a supposedly rigorous pilot regime have count results being manipulated in a standard office application makes a mockery of all the checks and controls that should be in place to ensure a legitimate and trustworthy election result.

Perhaps such problems would have been caught by a strict Quality Assurance regime but, as the Commission noted (6.44-6.52), the Government failed to provide an adequate level of assurance throughout the pilot process. Due to the short timescales the little work done was inconsistent and not conducted sufficiently independently of the suppliers. Furthermore, due to time pressures, much of the Quality Assurance work was completed during or after the election period thus preventing issues from being properly resolved. Those issues that were caught did not have time to be retested to ensure they were fixed thereby defeating the point of a Quality Assurance process. Additionally none of the findings that the Quality Assurance consultants did have time to write up were published undermining the creation of trust in e-voting. The Project strongly feels independent verification is needed if there is to be any hope of accepting the results of e-voting systems. The Government's remarkable response to these issues (pp24) was to argue that the short time scales for the pilots are inevitable to an extent but that as suppliers get used to them they will need less time to implement the e-voting systems! Despite this the Government has accepted the need for more consistent Quality Assurance throughout the pilots (pp21) and has committed to a better process for the next pilots, though makes no mention of publishing the results. The Project strongly urges the Government to recognise the specious nature of its arguments, there is little to indicate that repeated implementation of such major systems to short

timescales will alleviate the problems identified.

Unfortunately HMG (Her Majesty's Government) have placed themselves in somewhat of a bind as the current procurement framework prevents the creation of a single 'prime' contractor thus making future pilots unable to comply with the Commission's recommendation (pp10). It is disappointing that the Government set the contractual structures in stone and made such a basic error as to prevent simple lines of responsibility in what are complex IT projects desperately in need of clear leadership. One must also wonder what the point of a feedback process, such as the Commission's report, actually is if the framework has been set until 2005?

Technical & Security Issues

The 2003 pilots saw the first widespread use of a stable version of the EML (Election Markup Language) interoperability standard. The author welcomes moves towards interoperability (and avoiding vendor lock-in) through the use of EML, a standard whose development the Project was intimately involved with. However the Commission correctly noted (6.24-6.26) that interoperability risked opening security vulnerabilities at the interfaces between the different suppliers. Furthermore it was not clear how much compatibility EML's use actually offered, according to the Commission some interfacing problems were encountered and no independent testing of suppliers' compliance was offered. Despite this lack of testing or verification of EML compliance the Government places huge faith in this nascent standard for future pilots (pp16). Thus at the very least the Project feels that before basing an entire e-voting strategy on EML an assessment of the standard's performance and the vendors' compliance to EML during the 2003 pilots should be undertaken and made publicly available.

Security analysis during and after the pilots was lacking. While the Commission noted that some analysis of network and system log files has been undertaken (6.58-6.60) it rightly questions why no application level log files were analysed when they could reveal much wider fraud issues than the lower-level records assessed. The analysis at the time of the Commission's report was incomplete but again the Project

The uncertain nature of elections to come

must ask why the results have not been published and what steps were taken to protect the logs: The best cracker would naturally attempt to erase all traces of their attacks from log files.

The Commission states its desire to work with the Government to monitor and “investigate application-level events (such as log-in attempts) as well as network and system level events” in the next pilots. This is admirable but the Project questions the Commission’s competency in undertaking such a major task and wonders how easy it will be to draw together the vast quantities of information from the various suppliers in time for useful analysis or response without compromising the security and privacy of the voting process. This is a major technological challenge and the Project considers it highly unlikely that it can be achieved in time for the 2004 pilots as the Commission hopes.

The Commission’s position on protecting voter credentials and preventing vote selling is based on deterrence (6.61). Thus to improve the security surrounding credentials and to prevent their sale the Commission only recommends ensuring that stiff penalties exist and that the literature sent to voters clearly spells out the consequences of being caught. This seems to the Project to be a strange approach, if the Commission sees technology as being an acceptable tool in other aspects of the voting process why won’t the Commission examine a much more reliable method for protecting voters’ credentials than deterrence? The Project suggests that multi-use credentials are far less likely to be given, sold or lost by voters. This suggestion is not an endorsement of entitlement cards.

Despite the Commission’s useful recommendation that voting credentials should always be sent in two mailings HMG is cautious on this, citing usability difficulties (pp19), yet citizens are highly likely to be comfortable with such a process as it is exactly how they already receive their bank cards and PINs. Again on credentials the Commission makes the excellent recommendation that voting suppliers should not be involved in assigning voting credentials, thereby reducing the risk of a conspiracy within a supplier yet HMG will just “consider the practical implications” (pp19). In the Project’s view these two recommendations alone should be the minimum

The uncertain nature of elections to come

improvements made to credential security if e-voting pilots are to continue.

The Commission made several other excellent and detailed security recommendations (6.43):

- “the requirements should state that the linking information between anonymous credentials and voter identification should be held by organisations who are not involved in e-voting service delivery”
HMG will “consider further the detailed implications” of this recommendation.
(pp18)

The Project feels that this recommendation cuts to the heart of how secret electronic ballots are, it would be a considerable step towards establishing trust that votes and voters will not be linked unless ordered by a judge. Of course this ignores the issue of whether it is legal for votes to still be numbered in the UK which is a debate best kept for elsewhere but the question of whether, in the case of policy change, the systems being piloted could support truly anonymous votes must be asked.

- “the public verifiability requirements should be clarified”
HMG “regards the clarification of public verifiability requirements to be a key strategic aim, to be achieved step by step over a period of time.” (pp18)

The Project regards the Government’s response to this fundamental requirement as a meaningless fudge. Originally “publicly verifiable code” seemed to be the requirement but after much back-peddalling merely “public verifiability” remains. No government official or supplier has ever been able to clarify to the author what this was supposed to mean. The Project’s view is that if e-voting is to proceed then the full design and source code of election systems should be publicly available for assessment and review. Furthermore independent monitors should ensure that the systems used for actual elections are exactly that which have been published and assessed. Additionally ‘zero-counts’ at the start of elections to prove the counters are

The uncertain nature of elections to come

'empty' and voter-verifiable ballots should be in place to guarantee full verification of the election process. Indeed HMG agreed with the following Commission recommendation (6.36) only a page earlier (pp17): "The operation of the electronic voting scheme in relation to important electoral procedures should be documented clearly by the service providers so that electoral administration staff, candidates and agents are clearly informed about the processes that need to be followed. These procedures should include verifiable checkpoints and should result in an audit trail that can be used to verify that the election was conducted in a secure and robust fashion. This audit trail should be analysed and documentation should be produced to provide confidence in the correct conduct of the election. This documentation should be available to candidates and agents for inspection."

Not only does this recommendation indirectly provide damning criticism of the failings of the 2003 pilots' audit processes but, if the findings of such a process were published, would offer a bold step towards greater public verifiability. Thus the Government's equivocation on public verification is particularly troubling to the Project.

- "Specific and more proactive methods for measuring the number of attacks and level of potential fraud should be mandated for future pilots." *HMG agrees and will widen the analysis to cover all potential threats (pp10)*

While the Project agrees with the recommendation and the Government's response, it is astounding that specific methods have not already been in place to measure the levels of potential fraud during the 2003 pilots.

- "The use of multiple redundant hosting and infrastructure centres should be investigated in future pilots. This should be investigated when EML provides a sufficient level of interoperability between channels and hosting centres for this capability to be provided at a reasonable cost." *The Government doesn't leap at this recommendation merely stating that HMG "agrees that this is a strategic factor to be accommodated in the road map, reflecting*

The uncertain nature of elections to come

the conditions the Commission suggests.” (pp19)

Again the Project is stunned that no ‘hot failover’ sites were used during the 2003 e-voting pilots. Such continuity methods have been used in business for at least the last decade and it is highly surprising that such a time-critical and legally binding process as an election was not considered important enough to warrant such provisions. Indeed the Financial Services Authority wouldn’t allow a bank to trade without sufficient ‘hot’ backup systems, why should an election be any different? The Project is not clear what role EML would have in providing backup facilities and thus questions why EML’s development should be a restraining factor on mandating the implementation of proper backup and failover systems.

- “A full risk assessment should be undertaken for each e-voting service provided.”

HMG accepts this recommendation.

Once again the Project finds the need for the Electoral Commission to include this as a recommendation surprising and deeply disturbing. Comprehensive and detailed risk assessment should have been an integral part of the pilot process.

Usability Issues

The Project warmly welcomes the Commission’s recommendation and HMG’s agreement (pp21) that the user interface and terminology should be standardized for electronic voting (6.92), if e-voting is going to be implemented then it is highly desirable that disenfranchisement through poor design is avoided. The Project hopes that the relevant stakeholders will fully engage with the usability community to ensure the best possible practice is adopted. This standardization should also extend to the Internet domain names used for websites. The Project was surprised that no mention was made of the non-standard addresses used such as ‘voteyourway.org.uk’ which were illogical names open to spoofing. The .gov TLD

The uncertain nature of elections to come

should be used thereby ensuring registration is Government-controlled and, if appropriate, the appropriate region or constituency should also be in the address in a standardized manner such as 'vote.sheffield-hallam.gov.uk' or perhaps 'sheffield-hallam.vote.gov.uk' would be easier to administrate centrally.

Cost & Administrative Issues

According to the Commission (6.121) the funding provided by ODPM (Office of the Deputy Prime Minister) for electronic voting pilots came to £18,322,937 even though the Government had planned to spend only £10m for the year. However the Commission has made clear (6.122-6.124) that it was impossible to fully account for the total spending on the pilots due to the complexities of local authorities' accounting and the strange basis on which suppliers had to price their services with very little prior knowledge of the requirements. Thus the total amount spent on electronic voting is unknowable but considerably greater than the Government's £18.3m as local authorities also spent their usual elections budgets (at least) and many suppliers have privately admitted that they subsidised their services to ensure they remained competitive in the nascent e-voting market. The Commission concluded that "the cost per voter in these pilot schemes is an order of magnitude higher than in similar traditional elections" partly due to the immaturity of the technologies and procedures but the Commission argues, and the Project agrees that, "it is unlikely that the introduction of new electronic voting channels will provide cost savings while voting in person at the full range of polling stations is retained as an option" (6.120). Indeed despite the considerable sums of money being spent by central Government and local authorities the Commission felt that there was a lack of Government resources to "adequately manage" the pilots, as had been the case in 2002 (8.21). Additionally the Commission felt that "in general, there was a lack of technical expertise in e-government systems and IT procurement...which did cause a number of problems further down the line" and a lack of a formal mechanism to properly track the progress of suppliers and pilot implementation (8.21-8.22). The Government accepted these recommendations but it remains to be seen whether it will act on them.

The uncertain nature of elections to come

The Commission recommended that “to harness national publicity and actively promote using this method, all pilot Orders should require that voting channels are open until the close of poll.” (6.92). However the Government argued “that there are a number of practical and security issues to be considered, and solutions piloted where local circumstance permit, before the recommendation could be universally adopted.” The Project agrees with HMG that while allowing all channels to be active on the final polling day may be attractive in terms of convenience there are excellent security arguments for closing remote voting channels the day before to reduce the opportunities for double voting.

The bold new multi-channel world of electronic voting that the Government has put forward was rather diminished by the Commission’s view that text message and digital TV voting added little value and so future pilots using them should be kept to a minimum (8.5). The Project wholly agrees with the Commission that their value is questionable and furthermore that major security, privacy and usability challenges are raised by their use. However HMG seems to be fudging their response to the Commission’s recommendation stating that “The Government believes that the extent to which any particular channels are piloted in future must depend on the circumstances then prevailing, including the current state and take-up of technology, and the current priorities as identified from the road map at that time.” This response could mean pretty much anything and we feel that the Government is rather too wedded to the charms of new and exciting channels without giving due consideration to their true strengths and weaknesses, let alone their costs.

Finally both the ODPM and the Commission agree that the use of kiosks in polling stations do not offer significant cost benefits, despite this widely being seen as the most secure and reliable method of implementing electronic voting. Thus both are committed to focussing on remote electronic voting which is by far the most complex and risky class of electronic voting (pp12). By seeing all-postal ballots as being merely an intermediate step to remote electronic voting (pp8) not only does HMG risk failing to properly experiment with polling station e-voting but fails to recognise the significant legal and security problems with remote voting by paper or electronically. It is disappointing that both the Commission and the Government are

The uncertain nature of elections to come

choosing to underplay the problems of family voting, vote selling and vote stealing by focussing on remote voting methods. The doubts over the legality of voting from home raised by the European Bill of Human Rights also remain unresolved.

It still has not been made clear why voting convenience is important, particularly as both HMG and the Commission tenuously accept that technical improvements to voting will not have a major impact on turnout. The Project doesn't regard HMG, in particular, as wholeheartedly having relinquished the turnout arguments as they continue to discuss e-voting in terms of participation and involvement in political processes (pp5), leading the Project to believe that the pilots continue to chase a mirage of boosted turnout which e-voting continues to show it cannot deliver.

Conclusions

This analysis has shown that there were numerous serious failings in the planning, management and implementation of the pilots. The Government does not seem to understand the challenges involved in trying to build trust in electronic voting. Only by opening up the entire process and allowing detailed verification of all aspects of electronic votes can critics, candidates and voters begin to understand and trust the systems used and results declared.

The Government also seems to be repeating the same old IT project management mistakes: A lack of in-house expertise resulting in overly relying on suppliers to manage themselves and select technical solutions which may be sub-optimal but most profitable. Indeed e-voting does seem to be profitable for some with the Government overspending by around 80% and other spending impossible to account for.

The Electoral Commission's report has highlighted a muddled, rushed series of pilots which did not have proper security and fraud detection procedures in place. Voter credentials were often confusing and could be easily compromised when not sent separately. The voting systems were vulnerable to catastrophe as they lacked 'hot failover' backup systems. Counts were run in undocumented and highly insecure ways which risked undetectable abuse. A proper audit trail of voter and administrator use of the voting systems was not available while Quality Assurance was rushed and incomplete. Yes, the pilots ran, but it is a miracle nothing more disastrous than a few glitches occurred. Of course there remains the possibility that results were undetectably manipulated in one or more of the pilots, we shall never know but some councillors may be illegitimately wielding power.

While the Government has accepted many recommendations it has failed to wholeheartedly adopt some of the most important relating to verification and credential security. With the continued lack of in-house expertise, the already fixed supplier framework and the rapidly diminishing time until the next pilots the Project does not have huge faith that we will see significant improvements in time for 2004.

The Author

Jason Kitcat is an e-government and e-democracy expert.
For more information visit j-dom.org

Acknowledgements

The author would like to thank Ian Brown and Louise Ferguson for their contributions.

the free e-democracy project

SPRU, The Freeman Centre,
University of Sussex,
Falmer, Brighton
BN1 9QE
United Kingdom

www.free-project.org

+44 (0) 7956 886 508

© 2003 **the free e-democracy project**

Verbatim copying and distribution of this entire document is permitted in any medium, provided this notice is preserved.