

## Weekend Voting

### Response of the Open Rights Group and FIPR

#### Detail of Respondents

Prepared by: Becky Hogge

Responding on behalf of: The Open Rights Group (ORG)  
The Foundation for Information Policy Research (FIPR)

Address: Open Rights Group  
7th Floor  
100 Grays Inn Road  
London WC1X 8TY  
United Kingdom

Telephone: +44 (0)20 7096 1079

Email: [info@openrightsgroup.org](mailto:info@openrightsgroup.org)

Website: <http://www.openrightsgroup.org>

#### Response

The Open Rights Group (ORG) and the Foundation for Information Policy Research (FIPR) are appalled that the Ministry of Justice is considering the use of remote electronic voting. All our expertise and experience points away from adopting this technology. In this response, we seek to set out the significant risks remote electronic voting poses to our democracy.

E-voting is a uniquely difficult problem for computer science. E-voting systems must, with high assurance:

- Verify that you are eligible to vote
- Ensure that you vote only once
- Ensure you can vote anonymously
- Ensure you can vote privately
- Allow for meaningful recounts
- Allow for audit and oversight

There are currently no practical solutions which tackle all of these fundamental requirements simultaneously.

Evidence from elections in the UK and around the world shows that e-voting technology is vulnerable to significant error and fraud. 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. The testing, certification and audit processes designed and implemented so far have been quite unsatisfactory.

Voting is a uniquely difficult question for computer science and there are currently no practical solutions to this highly complex problem. Thus far, every commercial e-voting system evaluated by independent researchers has been found to contain fundamental security flaws<sup>i</sup>. Malicious or fraudulent attacks are not the only concern: errors caused by software bugs can also alter results. All election counts are affected by human error. But human error is random, and small scale. Introducing computers into the process means errors become systematic. If an e-voting system doesn't register any votes for one candidate, or counts backwards for one candidate whilst counting forwards for another, then the errors are not evenly distributed and the election result is no longer a fair representation of voters' intentions<sup>ii</sup>.

### **Remote e-voting**

In addition to the problems associated with electronic voting, remote electronic voting brings with it another set of issues. This is because systems based around the internet and PCs are vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc). These attacks may disrupt the process of voting or bring the results into question.

In this respect we note the conclusions of computer scientists David Wagner, Avi Rubin, David Jefferson and Barbara Simons, members of the Security Peer Review Group, an advisory group formed by the United State's Federal Voting Assistance Program to evaluate SERVE, an online absentee voting systems designed for the US military in 2004:

“We regret that we are forced to conclude that the best course is not to field the SERVE system at all. Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear. We want to make clear that in recommending that SERVE be shut down, we mean no criticism of the FVAP, or of Accenture, or any of its personnel or subcontractors. They have been completely aware all along of the security problems we describe here, and we have been impressed with the engineering sophistication and skill they have devoted to attempts to ameliorate or eliminate them. We do not believe that a differently constituted project could do any better job than the current team. The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the internet and the PC, or some unforeseen security breakthrough. The SERVE project is thus too far ahead of its time, and

should wait until there is a much improved security infrastructure to build upon.”<sup>iii</sup>

This advice led to US Government to abandon SERVE in 2004<sup>iv</sup>.

Further, elections held using remote electronic voting are vulnerable to manipulation of very traditional kinds, because it is difficult to verify that the voter is who they claim to be – and because others can watch the elector vote. This opens the door to voter coercion and vote buying. These have been a growing concern in the UK in recent elections as postal voting has become more widespread. Allowing online voting too can only make this problem worse, and further undermine trust in the democratic process.

With many systems, meaningful recounts are not possible as all the authorities have is a database of votes, with no paper trail for audit. We agree with renowned cryptographer and computer security expert Bruce Schneier, who has stated 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.”<sup>v</sup>

### **A black box system**

Electronic voting systems are of various kinds, including equipment that automatically scans and counts paper ballots, and direct recording equipment (DRE) that simply keeps an electronic tally. For online operation, it is most likely that DRE e-voting technology would be chosen. But this technology operates as a “black box”: voters, candidates and even officials cannot see the inner workings of the machines. Only a small group of technology experts has any hope of understanding how the election is being conducted and counted, and even then, the scrutiny required from such experts would not be trivial: manipulating bits in a computer is much easier than copying paper ballots, so there is potential for hard-to-detect vote manipulation on a scale never seen before. A hacker could hide a tiny piece of code in the voting software that could significantly modify an election’s results.

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<sup>vi</sup>, or where the system failed, complicating access to and occasionally depriving people of their right to vote<sup>vii</sup>. Problems are often not discovered until the election is over, when it is impossible to put matters right.

Unlike with paper ballots, when problems occur, there is little for election officials to study. 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<sup>viii</sup>.

These risks are exacerbated by e-voting suppliers' insistence on commercial confidentiality for 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 serious security flaws. Secrecy does not serve the integrity of our elections. In this respect we note the inability of London Elects to release an independent audit conducted by KPMG on electronic vote-counting software used in the London elections in 2008, because of vendor (and auditor) concerns over commercial confidentiality<sup>ix</sup>.

### **The risks outweigh the benefits**

Transparency of elections is a vital ingredient for public trust in the electoral process, as well as of the integrity of the process itself. When government considers how to raise public participation in elections, the first thing to consider is how to ensure that elections make a difference. If they're perceived not just as being ineffective in most constituencies, but also rigged, then participation is likely to fall still farther.

There are those who suggest that e-voting is inevitable and that to oppose the technology would be Luddite. Politicians and commentators who are afraid of technology may be cowed into silence by this thoroughly dishonest argument. We will not be cowed. ORG and FIPR number many computer scientists and engineers among our members and supporters. We say, loud and clear, that elections are one of the last processes in Government that should be automated. The risks are huge, the rewards are nugatory, and the experience of overseas pioneers is frankly dreadful.

## **The May 2007 Experience**

The Open Rights Group fielded a volunteer team of officially-accredited election monitors to observe the use of e-voting and e-counting technologies in the May 2007 elections. The reports on the May 2007 elections by ORG and the Electoral Commission both found considerable problems which bring into question any further use of all computer mediated voting technology. The procurement and management of the systems was inadequate and costly, and the Government indicated a lack of understanding of the nature and scale of the problems e-voting can introduce into the electoral system.

We repeat a summary of ORG's observations of the May 2007 elections specific to remote e-voting below, but recommend that all now considering the so-called "modernisation" of elections read ORG's reports into the May 2007<sup>x</sup> and May 2008<sup>xi</sup> elections, and we incorporate them here by reference.

In Rushmoor a remote electronic ballot displayed incorrectly at the opening of advanced voting and electors reported problems with error messages. Online voters in Sheffield also had trouble casting their votes. Where they existed, cryptographic receipts were generally poorly designed and difficult for voters to use.

Though some newer remote-voting channels such as telephone voting may appear superficially attractive to groups of voters such as the elderly and housebound, in practice these were the very voters who appeared to experience most difficulties. ORG received a number of reports concerning difficulties in understanding and using the telephone voting system in South Bucks, and in understanding the registration process in South Bucks and Rushmoor. There was no evidence that usability testing had been conducted to ensure processes were as easy to use as possible. Voters in South Bucks, who had registered for remote voting, but then experienced difficulties, were prevented from voting in person at polling stations. These voters were effectively disenfranchised.

## **About the Open Rights Group**

The Open Rights Group is a grassroots technology advocacy organisation, founded in 2005. Our core operations are funded by hundreds of tech-literate UK citizens who want their voices heard in national debate around technology issues. We speak out against the poor regulation and implementation of digital technology. We aim to protect and promote civil, human and consumer rights in the context of digital technology.

## **About the Foundation for Information Policy Research**

The Foundation for Information Policy Research is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

- i For the most recent example of this, see the University of California, Santa Barbara's Top to Bottom review of the electronic voting systems used in California, available at <http://www.cs.ucsb.edu/~seclab/projects/voting/> Also see <http://avirubin.com/vote/analysis/index.html>
- ii For more on these issues, see <http://www.wired.com/politics/security/commentary/securitymatters/2006/11/72124>
- iii See <http://servesecurityreport.org/>
- iv See [http://www.theregister.co.uk/2004/02/06/pentagon\\_cans\\_internet\\_voting\\_system/](http://www.theregister.co.uk/2004/02/06/pentagon_cans_internet_voting_system/)
- v See <http://www.schneier.com/crypto-gram-0012.html#1>
- vi See *Hacking Democracy* <http://www.hackingdemocracy.com/>
- vii See ORG's report into problems in pilots in England in 2007 ([http://www.openrightsgroup.org/wp-content/uploads/org\\_election\\_report.pdf](http://www.openrightsgroup.org/wp-content/uploads/org_election_report.pdf) )
- viii See <http://www.hackingdemocracy.com/>
- ix See [http://www.londonelects.org.uk/resources/kpmg\\_audit\\_reports\\_tcs.aspx](http://www.londonelects.org.uk/resources/kpmg_audit_reports_tcs.aspx)
- x See [http://www.openrightsgroup.org/wp-content/uploads/org\\_election\\_report.pdf](http://www.openrightsgroup.org/wp-content/uploads/org_election_report.pdf)
- xi See <http://www.openrightsgroup.org/wp-content/uploads/orglondonelectionsreport.pdf>