STATES OF JERSEY

PUBLIC ELECTIONS: ELECTRONIC VOTING

Lodged au Greffe on 18th February 2016
by Deputy G.P. Southern of St. Helier

STATES GREFFE

PROPOSITION

THE STATES are asked to decide whether they are of opinion –

to request the Privileges and Procedures Committee (PPC), in conjunction with the Comité des Connétables, and other government bodies as appropriate, to research and trial electronic voting systems in order to introduce –

(a) methods for electronic voter registration; and

(b) safe and secure mechanisms to enable eligible voters, who wish to do so, to vote electronically,

in the 2018 elections.

DEPUTY G.P. SOUTHERN OF ST. HELIER

REPORT

I start this report with 2 short statements delivered by the Chief Minister to the KPMG Islands' Group Conference in 2015 on e-government and digital initiatives –

> "*We are reprioritising our spending so we can put the money where we really need it, and* ***offering more services online is integral to these plans****. We have already set up systems for e-government which are providing a solid foundation for some of the more technical elements of the programme. Now we are now focusing the e-government programme on getting our tax and Social Security systems to share information and on enabling teams and departments to work more closely together.*
>
> ***Our aim in e-government is to deliver quality services*** *re-organised around our customers.* ***This will support the drive to make the public sector more efficient.***".

He went on to confirm his commitment with the creation of a new post –

> "*I have given my Assistant Chief Minister responsibility for the Financial Services and Digital Industries, Competition and Innovation. Senator Philip Ozouf is working hard to create the right conditions to foster economic growth, to support increased productivity in all parts of the economy and to encourage new business start-ups across different sectors.*
>
> ***We are looking for new and innovative ways to do things better by embracing technology****, diversifying the local economy and creating rewarding job opportunities that build a good standard of living for islanders****. We are putting a greater emphasis on innovation and technology.****".*

What better way to demonstrate and to advertise to the world our commitment to digital innovation and e-government than to bring our election system into the 21st century?

A survey of the literature on the subject of e-voting reveals that many of the stakeholders concerned are supportive in principle, usually in terms of increasing voter turnout, but adopt a wait-and-see approach in the light of reservations concerning security and potential fraud.

In September 2014 the Political and Constitutional Reform Committee of the House of Commons published a report entitled "Voter engagement in the UK – Political and Constitutional Reform". The report examined voter registration and turnout, pointing out the continuing decline in electoral participation in the UK –

> *"Although turnout for the 2010 general election was the highest for any general election since 1997, the number of registered voters that did not participate – 15,909,857 – was still larger than the turnout for any one party. When the number of people eligible to register to vote but not correctly registered to vote, are reckoned in the total, the number of people that did not participate at the most recent general election is larger than the number of votes cast for candidates of the two largest parties, or of both of the Coalition parties.".*

The comments contained in the report about the health of the UK democratic process could equally apply to our own –

> *"Democracy is working less well than it used to and we need to move swiftly to pre-empt a crisis. The scale of the response must be equal to the task. Millions of people are missing from the UK's electoral registers. Many of those who are registered – and in many cases the majority – choose not to participate at elections, be they for the UK Parliament, local government, or the European Parliament. In a modern democracy, it is unacceptable that millions of people who are eligible to vote are missing from electoral registers. We believe it should be made clearer in law that any person who is eligible to vote in a UK election should be on the electoral register. We also believe that it is desirable in a representative democracy for turnout at elections of all kinds to be higher – and ideally far higher – than has been the case in recent years*.".

The following is an extract taken from the 2014 report –

> **"Modernising electoral administration**
>
> 145. There are several ways in which current electoral practices could be modernised to make voting more accessible to the electorate, and we have been told that "the more opportunities provided for individuals to vote, the more likely they are to do so". Phil Thompson, Research and Evaluation Manager at the Electoral Commission, told us of some views the Electoral Commission had received from the public in a recent opinion survey. The results included:
>
> 70% of people said they would support weekend voting;
>
> 65% would support advance voting in some other way so voting would be stretched over a number of days, and
>
> About 63% of people said they would support the introduction of online voting.
>
> Between 2000 and 2007 several electoral modernisation pilot schemes were run across the UK, but none have been run since.".

The report examined the following options –

- Weekend voting – a 10% increase in turnouts
- Extended voting – we have already adopted with pre-poll voting
- Polling day to be a bank holiday – debated and rejected by the States
- Voting in any polling station – requires an electronic register
- Online voting.

Online voting

The core of the report concentrated on online voting, reproduced here –

> "151. We have received a significant amount of evidence in favour of online voting, whereby voters could cast their vote over the internet. Several submissions from members of the public and civic groups supported the idea, or stated that it would have a positive impact on participation. Others raised concerns about the possibility of fraud, and difficulties around guaranteeing secrecy. Phil Thompson, Research and Evaluation Manager at the Electoral Commission, told us that in a recent survey "half of the people who didn't vote told us they would have been more likely to vote if they had been able to vote online", and the written evidence from Lodestone also indicated that online voting could be particularly effective at engaging those people who do not currently vote, as their survey of non-voters found that "67% of those who didn't vote in 2010 said that they would be more likely to vote if they could vote online".
>
> 152. The National Union of Students stated that online voting "presents a good opportunity to ensure that democratic processes better reflect the practices that young people and students already utilise", and Toni Pearce, President of the NUS, also told us: "One of the reasons that online voting is so attractive for me is not just about encouraging young people to vote but the issue of access, particularly for disabled people, for being able to vote."
>
> When we took evidence from the University of Sheffield Students' Union, we heard about how they had moved to a system of online voting for Union elections in 2009. Online and paper voting were run concurrently in 2009 and 2010, but as few votes had been cast by paper in 2010 elections had been exclusively online since 2011. The impact on turnout had been significant, with an increase in the number of people voting of over 50% in the first year elections were run online, and turnout increasing further with each subsequent year. When surveyed, 85% of students at the University of Sheffield said they would be more likely to vote in governmental elections if they were able to do so online.
>
> 153. Dr. Toby James told us that online voting was something he could give "lukewarm support" to, as "evidence has not shown it bringing about a major increase in turnout yet". That said, he also told us that "times are changing and it is something we should certainly keep under review". He did give some suggestions for situations which could encourage greater take up of online voting, when he referred to previous pilots in 2003, stating: "what we did see from those pilots was that where you had internet voting in place in consecutive elections, more people began to use it. If you had internet voting open until the close of the poll, at 10 p.m., more and more people would use it." We also received written evidence from Rushmoor Borough Council, which was involved in the previous pilots of online voting, outlining the results of the pilots and suggesting some ways in which future pilots could be improved. Their experience was that online voting did not meet their targets for

increasing turnout, but was generally received positively by people who used the system.

154. Concerns we heard about online voting centred on risks of electoral fraud and problems in guaranteeing secrecy of the ballot. Professor R.A. Watt stated that "new (i.e. digital technologies) are not suitable for introduction into the remote voting (unsupervised, out of polling station) environment" as there would be issues around fraud and the secrecy of the ballot if people were allowed to vote digitally outside of a polling station. A written submission from Policy Exchange stated that online voting could trivialise elections, and that it was also "arguably […] inconsistent with the core principle of the secret ballot."

155. In terms of how online voting could be taken forward, Democratic Audit told us –

> 'We think we should definitely have a sustained, serious experiment of using online voting on a larger scale than has been tried before.'

Fran O'Leary told us:

> '… we believe that there should be closer interaction between Government, industry and academics to ensure that any internet voting systems that are developed are safe, secure and economical.'

However, it does not appear that the current Government are planning to implement changes such as online voting. When we questioned Sam Gyimah MP about various proposals that might improve voter participation, he told us:

> 'Looking at the options that are there, you have widening the franchise, electronic voting, weekend voting, all of these have been suggested a number of times over the years. In my view there are more downsides than upsides.
>
> […]
>
> There are some good arguments for them but I think at the moment the downsides outweigh the upsides, but then you would not have talked about online registration 10 years ago so you never know, their time may come.'

156. **Online voting is a proposal for increasing levels of participation that has received strongest support from our witnesses, although support has not been unanimous. Enabling electors to cast their vote online if they choose to do so would make voting significantly more accessible. In light of the move to IER, and the already high take up of postal voting, there is scope for giving online voting further consideration, although this would need to be balanced with concerns about electoral fraud and secrecy of the ballot.**

We believe that online voting could lead to a substantial increase in the level of participation at UK elections, and we recommend that the Government should come forward with an assessment of the challenges and likely impact on turnout, and run pilots in the next Parliament with a view to all electors having the choice of voting online at the 2020 general election."

[…]

"CONCLUSION

162. **Given its importance to our democracy we feel that there is a need to revisit electoral administration on the basis of convenience for electors and no other interest. Several changes, which have in the past been of academic interest, including online voting, holding elections on weekends or over several days, having a "Democracy Day" public holiday for voting, letting voters cast their vote anywhere in their constituency and having all-postal votes, are now measures which need to be considered in the context of improving voter participation. There is compelling evidence that some of these changes could have a substantial, positive impact on the levels of voter participation. Particularly if taken together, these changes could demonstrate that "the powers that be" are serious about voter engagement.**

We recommend that the Government, working with the Electoral Commission and EROs, bring forward a package of reforms to electoral arrangements to increase accessibility and turnout, and establish a series of pilots early in the next Parliament to test the various proposals that we have considered, with a view to making permanent changes to electoral arrangements by 2020.".

Speaker's Commission on Digital Democracy

The committee's conclusions received immediate backing from the Report of the Speaker's Commission on Digital Democracy in January 2015 –

"The Commission is confident that there is a substantial appetite for online voting in the UK, particularly among young people. It will become increasingly more difficult to persuade younger voters to vote using traditional methods. It is only a matter of time before online voting is a reality, but first the concerns about security must be overcome. Once this is achieved, there will be an urgent need to provide citizens with access to online voting, and the UK must be prepared for this. The Electoral Commission has called on the Government to introduce a "comprehensive electoral modernisation strategy […] setting out how the wider use of technology in elections will ensure the achievement of transparency, public trust and cost effectiveness". The new online registration system could be a cornerstone of a future online voting system, although it would not solve the problem of verifying the identity of people when casting their vote online.

We support the draft recommendation of the Political and Constitutional Reform Committee on Voter Engagement in the UK, urging the introduction of online voting by 2020. We agree that this would make voting significantly more accessible. However, we also agree that concerns about electoral fraud and secrecy of the ballot would need to be addressed first.

In the 2020 general election, secure online voting should be an option for all voters.".

Voter Security

While all these reports are convinced that the introduction of electronic voting will increase turnout, especially amongst the young, they contain repeated reservations concerning the issue of security of the ballot and the possibility of fraud. These issues exist with all methods of distance voting, including postal voting, a problem which in Jersey has been solved for many voters, including those with a disability, by the adoption of pre-poll voting at several sites and in the home. However, examination of this issue shows that there are a number of routes to potential solutions. With increasing numbers of the population happy to bank online or even by telephone, it must surely only be a matter of time before online voting becomes both widely accepted and safe. For example, work being undertaken at Birmingham University in 2015 has received widespread coverage, including this, taken from the WebRoots Democracy publication on secure online voting –

"**University of Birmingham 'Du-Vote' system**

In May 2015, computer scientists at the University of Birmingham claimed to have made a 'breakthrough' in secure online voting technology, developing a technique to allow people to cast their election votes online even if their computers are suspected of having viruses. Led by Professor Mark Ryan, the researchers took inspiration from banks and created a system which allows people to vote by employing independent hardware devices in conjunction with their PCs.

The researchers claim the system could be ready for use in the 2020 or 2025 General Election.

> *"This system works by employing a credit card-sized device similar to those used in online banking. It is called Du-Vote, and we have been developing it over the past two years. From the voter's perspective, it's straightforward: you receive a code on the device and type it back into the computer.*
>
> *The main advantage of this system is that it splits the security between the independent security device and a voter's computer or mobile device. A computer is a hugely powerful, all-purpose machine running billions of lines of code that no one really understands, whereas the independent security device has a much, much smaller code base and is not susceptible to viruses."*

The most comprehensive report on the issue of secure online voting comes from WebRoots Democracy, referred to above, published on 26th January 2016. It concludes that –

> ***"Online voting can be made sufficiently secure and should be introduced for the 2020 UK General Election."***

The report, backed by MPs from across the political spectrum, is written by global experts and academics in the electronic voting field, and examines the key security challenges facing the implementation of online voting for UK elections.

The report covers areas such as cyber-attacks, voter coercion, and malware on devices.

The 30,000 word document is made up of contributions from e-voting experts from the UK, USA, Spain, and Estonia, including UK-based companies – Electoral Reform Services, Mi-Voice, and Smartmatic, as well as computer scientists Dr. Kevin Curran from the University of Ulster and Professor Robert Krimmer from Tallinn University of Technology.

Each of these bodies examines the progress that has been made, along with work that needs to be addressed, on up to 12 key security issues which are critical in producing safe and secure online voting. I strongly recommend that members read the whole document, but I reproduce, in the **Appendix** to this report, the section from UK Electoral Reform Services, who have enormous experience in running elections at all levels.

Financial and manpower implications

As a first stage in developing an online voting system, the emphasis must be on research and evaluation trials. The review of 4G Spectrum cost £30,000 in 2012; whereas evaluation of Jersey Enterprise only cost £11,000. I estimate that equivalent research from a relevant adviser might be undertaken on a budget of around £20,000. If this sum cannot be found from the PPC budget over the next 2 years, then it should be allocated from contingencies. There should be no additional manpower requirements.

APPENDIX

"**Electoral Reform Services**

About

Electoral Reform Services (ERS), based in London, was born out of the campaigning organisation, Electoral Reform Society, in the 1980s.

Last year, over 400 organisations throughout the UK conducted electronic ballots with ERS – whether online, by telephone, or by text.

They are experienced in running elections and providing online voting services for professional bodies, companies, and political parties including the Conservatives, Labour, and the Liberal Democrats.

They notably co-ordinated the 2015 Labour leadership election which was the largest online voting election in UK history with almost 350,000 votes cast online.

Voter verification

Different methods of authentication can be used to enable voters to cast their electronic votes, e.g. single-use "security codes" or personal ID information such as dates of birth or national insurance numbers. In countries where electronic ID cards are already being used to facilitate access to health services or banking (e.g. Estonia), these can also be used to digitally sign the vote. An electronic voting system must be able to identify that the information being provided to authenticate the voter is the information required to enable a vote to be cast and recorded in that particular ballot and it must be unique to the voter.

The vast majority of organisations working with ERS will issue (by post or email) their voters with randomly generated single-use security codes to enable them to access the electronic voting systems. This is similar to a postal ballot, where a ballot paper number is used to make the ballot paper unique. Other organisations have required voters to provide personal identifiers such as dates of birth, and postcodes (online or by text) or a membership number and a date of birth.

Safeguards from peer-pressure

We discussed above how electronic voting information and security codes can be distributed to the voter by various means and that there are risks associated with any transfer of information that requires a third party carrier. Once delivered, the vote cast must be secret. There is good practice advice for voters on how to cast their vote in secret – often basic advice such as considering their physical location when they cast their vote and the proximity of others to them.

The risks of vote coercion and vote selling (for example a company could bribe or threaten its employees to vote in a certain way, or a landlord threaten their tenants) also need to be addressed. This risk arises with any form of remote voting including postal ballots or online, telephone and SMS voting. Legislation, with appropriate penalties such as fines or prison sentences, will provide some safeguard against this risk. Another possibility is to allow voters to vote multiple times, with only the last vote being

counted. A vote-buyer is unlikely to pay you for your online or postal vote if they know you could later change it online or at a polling station. There are also various techniques which allow a voter to obtain a receipt for their vote, which proves to the voter that their vote has been cast in a certain way, but which would not be accepted as proof by a vote-buyer. This is an active field of research by cryptographers.

Ensuring the correct vote is submitted

It is possible to provide voters with the opportunity to independently check if their vote has been received and how it has been recorded. This is known as a voterverified audit trail (VVAT). This can be setup in various ways for example by allowing voters to log in and check their receipt on a website "bulletin board", or phone a telephone service to confirm the vote or even get a separate postal receipt sent to a personal postal address. For contentious and high profile ballots the use of VVAT may be an added security measure that enhances the integrity of the ballot.

As mentioned above, cryptographic methods may be used to ensure the voter's receipt does not facilitate coercion or vote-selling.

Ensuring the correct vote is received

Again there is a risk with any form of remote voting that the vote might be tampered with after submission but before receipt by the organisation counting the votes.

Imagine a postal worker steaming open your postal ballot and altering your vote before putting it back in the post. With online voting this risk is largely addressed by configuring servers to require secure (https) connections, this forces traffic between the browser and server to be encrypted so it cannot be altered during transmission.

The use of Extended Validation (EV) SSL/TLS certificates gives the voter greater reassurance that they are submitting their vote to the correct website (an EV certificate is only issued to a website owner after vetting by the certifying authority).

Safeguards against malware on the voter's device

With personal devices there is always a possibility that malicious software is present. If designed specifically in relation to a ballot it could disrupt, change or read and communicate to a third party the voter's vote. Whilst anti-virus software exists, it must be kept up to date and can only protect against known issues. It is important here to ensure voters are aware of the risk of using electronic devices and maintaining personal data security. For example, keeping authentication codes secret, not clicking suspicious links or opening attachments in unexpected emails, and appropriately deleting and destroying voting information.

Safeguards against cyber-attacks

The system should be built and configured according to recognised industry guidelines, such as the server-hardening standards published by the Centre for Internet Security (CIS). The system should also be regularly scanned for vulnerabilities by independent third party such as an ASV (Approved Scanning Vendor i.e. an organisation with internet security expertise which has been approved to conduct testing for compliance with the PCI DSS standards for credit card processing).

Infrastructure supporting the systems should be robust and mitigate against downtime or interruption of service, for example through the use of redundant architecture and system replication. Online voting providers must be able to demonstrate that they have rigorous quality assurance procedures and processes. Evidence such as certification in quality management and information security, e.g. ISO9001 and ISO27001 would be expected.

Contingencies in case of vote-tampering

Suspicious activity needs to be investigated as described below, and if there is evidence of malpractice voters would be invited to cast their vote again. If a multichannel voting system is used (e.g. if voters can choose to vote online, by post or in person) it also offers the opportunity to compare voting patterns between channels. Depending on the risk assessment for each channel, a threshold or limit could be placed on votes allowed via that channel e.g. elections could include online voting provided no more than 30% of votes are cast online (similar thresholds are currently being used in Switzerland, with the intention of gradually increasing the threshold as and when security requirements are met).

Detecting interferences with the online voting system

ERS has been running postal ballots for over 100 years, and online votes for over 15 years. We currently administer around 2,000 election projects each year, each project may have multiple contests and constituencies, which requires many thousands of individual ballots. As such we have acquired a great deal of experience of monitoring the pattern, timing and frequency of votes being cast, internet protocol (IP) addresses, etc., so that suspicious activity can be investigated for evidence of malpractice.

Maintaining audit trails

It should be possible to audit that any submitted vote is correctly included in the count and has not been altered whether by malware on the voter's computer, hackers intercepting traffic between the voter and the webserver, or even corrupt employees at the online voting vendor with access to the stored votes. Ideally the audit should be carried out by the voters themselves although this will be an unfamiliar process as the audit and assurance is currently carried out by other means. For example a trusted independent body running the election, or political party agents being allowed to witness the sorting and counting of ballot papers on election night. The value of any audit depends on a sufficiently large sample of cases being audited, so voters will need to become familiar with these new processes in order to carry out the audits in sufficient numbers to provide the necessary reassurance in the integrity of the vote.

Ensuring the system is sufficiently secure

Load-testing is an essential phase in the development of online voting sites which need to be able to cope with very high peaks of traffic particularly at the beginning of the voting period immediately after polls open and again just before polls close. ERS has experience in administering online voting projects for some of the largest organisations in the UK, including trade unions, political parties, and building societies and other financial institutions, so we have acquired detailed knowledge of patterns of turnout over the voting period. It might be acceptable for commercial websites, such as those

selling event tickets, to hold customers in a queue when the servers get too busy, but this would not be ideal for online voting as voters might just give up and reduce turnout.

Security testing is also critical for the success of an online voting site. ERS' in-house development team will conduct application security tests as part of the development process, but we will also commission an independent third party specialising in web application security to test major releases of our software.

Internet security can seem like an "arms race" between developers and hackers, every time a developer fixes a bug or vulnerability, some hacker will discover a new one. It is therefore essential to ensure that experts with the most up to date knowledge of internet security have tested the system.

Securing voter records and personal details

It is good practice to separate, physically and electronically, the system and database used for the distribution of the voter information from the database used to store the votes cast on the electronic voting system. The only commonality between these two systems being the authentication codes used by the voters. This ensures that the voter's identity is separated from their voting preference but, as currently with UK public elections and other postal ballots, this allows, in the event of queries or challenges, for the online voting provider to investigate and if need be invalidate the votes from a particular voter.

It is also possible for the data related to the ballot to be encrypted when stored to further enhance the security and secrecy of the vote, however this is not as straightforward as it sounds. If the data has to be searched or any calculations performed (such as vote-counting), then any encryption can impact performance and make the system unusable. Techniques such as homomorphic encryption (allowing votes to be counted without decryption) have been developed and may be used on certain types of ballot, but this is another active field of research by cryptographers.

Open-sourcing and working in an alliance

ERS is happy to work in alliance with others and has done so for several public voting and vote-counting projects in the past, including previous pilots of online voting in the UK. Our own software is currently not open source and this is an open question. On the one hand if the code is open source then it gives any would-be hacker full knowledge of how the software works, which might allow them to construct malware specific to that voting system. On the other hand making the code open source means it can be reviewed by a wide audience and give voters greater re-assurance that the software is fit for purpose."