Electronic Balloting Review

The Report of the Independent Review of Electronic Balloting for Industrial Action

Sir Ken Knight

DEPARTMENT FOR BUSINESS, ENERGY AND INDUSTRIAL STRATEGY

Electronic Balloting Review

The Report of the Independent Review of Electronic Balloting for Industrial Action

Presented to Parliament pursuant to Section 4 of the Trade Union Act 2016

The conclusions and recommendations in this report are those of the author and do not necessarily represent the views or proposed policies of the Department for Business, Energy and Industrial Strategy.

Contents

Foreword

I was asked by the Secretary of State for Business, Energy and Industrial Strategy to carry out an independent review of electronic balloting (e-balloting) for industrial action ballots. The Terms of Reference (at Annex 1) required that I considered the key factors which would contribute towards a robust e-balloting regime. The key requirements were that I took into account the following issues:

- The electronic and physical security of e-balloting methods, including risks of interception, impersonation, hacking, fraud or misleading or irregular practices;

- If any system can safeguard against risk of intimidation of union members and protect anonymity of ballot responses;

- The security and resilience of existing practices of balloting of union members;

- The aims of the Trade Union Act 2016 to ensure strikes and related disruption to the public only happens a result of a clear, positive decision by those entitled to vote.

I was pleased to undertake the review as after 40 years in the Fire and Rescue Service I have considerable experience of industrial disputes and labour relations issues. More recently, as the Commissioner for Tower Hamlets I have first-hand experience of what can go wrong with ballots where there is a lack of transparency and the potential for intimidation and consequential impact on the trust and cohesion on which a ballot relies.

I am extremely grateful to all those who have attended meetings in connection with this review and have responded to my Call for Evidence and for the technical support from the cyber experts whose report is included in this report. Lastly, I would especially wish to thank the small team of officials at BEIS for their assistance and support.

In recommending that e-balloting be tested, the report reflects my view that there is potential to examine in practice, whether this can be an effective option for Government and trade unions to ensure that ballot results are a true reflection of the views of those entitled to vote by increasing the turnout at elections. However, the decision is by no means clear cut and, for a number of reasons, I have recommended that e-balloting be tested in the context of non-statutory balloting over a reasonable period - to be decided by the Secretary of State. The purpose of this should be to examine its reliability, not least the need to be certain that the technology is capable of withstanding cyber-attack, not only by nation states, but also those who may be motivated by the desire to disrupt and deny services and thereby damage vital trust in industrial relations.

I believe this report contributes constructively to the industrial relations debate and I hope it will be helpful to the Secretary of State in deciding the way forward.

Sir Ken Knight CBE QFSM

Executive Summary

In November 2016 the Government announced that it was commissioning an independent review of e-balloting for industrial disputes. I was appointed to conduct the review and I issued a Call for Evidence, which prompted a good response. I have also met a large number of interested parties, including the Confederation of British Industry and individual employers as well as the Trades Union Congress and individual trade unions.

I conducted a number of roundtables with key stakeholders. There were five in all, including one in London, one in Cardiff and one in Glasgow. These three sessions were of a general nature and open to employers, trade unions, scrutineers, technology providers and cyber experts to attend. In addition there were two other roundtables, one for employers and another for trade unions. To learn from others' experience, I visited Estonia to see how e-balloting works there and also met a number of experts including the Electoral Commission, Electoral Reform Services Limited, trade union members, and representatives from Denmark. I also discussed e-balloting with the National Cyber Security Centre.

To ensure there was a firm technological base to my review, following an open tender, I commissioned a technology assessment report from cyber experts Professors Mark Ryan (Birmingham University) and Steve Schneider (University of Surrey). Their report is published at Annex 4 in this document.

During my review I was clear that my task was not to focus on the most significant examples of democratic balloting in modern society and the standards that would be required for a general election, local election and referenda. However, ballots for industrial action in public-facing industries are by no means at the other end of the balloting spectrum. I consider, in particular, that industrial action ballots in the public-facing sectors need to satisfy constituents that the result is fair, representative and trusted. Those needing to feel confident in the system include: the individual trade union member, the trade union, the employer and the public affected by any action that ensues. This context is reflected in my findings, together with the necessity for individual e-ballot decisions to be entirely secret, and protected accordingly.

A number of contributors have made the point that the existing postal ballot arrangements can be subject to abuse so are less than perfect and that a test for e-balloting is that it should be no worse than the existing arrangements. I accept this. But the point for me is that e-balloting in the context that some are proposing to use it is not yet sufficiently tested and assured. To move ahead without that assurance runs a real risk of e-balloting being found to be flawed and therefore not trusted. There are a number of respondents who argue that it is time to move quickly to this form of voting. I understand that position. However, I am equally aware that an early failure would cause significant disruption arising from flawed ballot decisions and would be likely to trigger the withdrawal and delay of e-balloting for many years.

Having held detailed discussions with those most involved in balloting in the context of my review and having examined the evidence received in response to my Call for Evidence, I believe it is appropriate to test whether e-balloting is a secure and reliable enough option to sit alongside postal balloting as a method of balloting for industrial action.

At first glance electronic voting may well appear to be the best modern method of reaching important decisions quickly and efficiently. However, voting in the context of industrial action is a very serious matter and must be handled responsibly. There are a number of aspects of e-voting to be considered and these are detailed in this report.

In a period in which we are experiencing increased allegations of cyber-crime, whether it is hacking by nation states or delinquency by those motivated to disrupt or damage civil society it is particularly important to evaluate how practical and secure this method of voting is. We need to be assured that it is not only capable of producing a valid result that voters, trade unions, employers and the public can have confidence in, but that it is robust enough, so will not be found wanting or inoperative when it is required to deliver.

Measures also need to be considered to avoid e-balloting being more open to coercion or undue influence than might be possible under the existing postal voting method. Accordingly, I consider that e-balloting needs to be examined in test conditions before it is introduced under any live situation or fully rolled out. I conclude that the method should be tested in non-statutory ballot situations for a period to be decided by the Secretary of State. A thorough evaluation should then be carried out which the Secretary of State can consider.

I now present the Government with my recommendations, which are based on the conclusions listed on pages 52-55.

My specific recommendations to the Secretary of State are below:

Recommendation 1: E-balloting for industrial action ballots would only be capable of retaining public confidence if it were seen to be as secure and reliable as the current postal approach. In particular, e-balloting would need to be able to meet the required standard set out in Section 54 of the Employment Rights Act 2004; i.e. it would need to ensure that those entitled to vote had an opportunity to do so; all votes cast would have to be secret; and the risk of any unfairness or malpractice would have to be minimised.

Recommendation 2: Owing to the number of unanswered questions surrounding e-balloting I am not persuaded that e-balloting for industrial action ballots can be introduced immediately. Instead I recommend that a test of e-balloting on non-statutory ballots is necessary as a preliminary step and that this would potentially be the basis for the Secretary of State to decide the matter.

Recommendation 3: Specifically, e- balloting should be trialed to see if it can meet the standard set out in Section 54 Employment Rights Act 2004. E-balloting should be introduced for selected non-statutory ballots across England, Scotland and Wales with the aim of evaluating, at least, the following:

- The resilience of e-balloting systems to cyber-attack and hacking. In this respect it is appropriate to use “ethical hackers” to test the robustness of systems used to support voting during any e-balloting trial;

- The operation and effectiveness of voter verification (the ability of voters to check that their vote has been received and cast according to their wishes);

- The alternative hardware options for casting a vote, including smartphones, emails, computers and, if appropriate, employers' IT systems;

- Whether having 're-voting' (multiple voting, last vote counts) provides increased protection from ballot malpractice and permits a period of reflection up to the close of ballot;

- Whether there is increased participation in a ballot as a result of e-balloting;

- How e-balloting might impact on people with disabilities as compared to postal ballots;

- The benefit of independent audit/assurance;

- Amendments that may be required to the BEIS approved scrutineer list to accommodate e-balloting;

- What additions might be needed to the code of practice for industrial action ballots to take account of e-balloting.

Recommendation 4: The providers of any systems used to trial e-balloting must be able to demonstrate that they are able to withstand cyber-attack/hacking from those who wish to cause disruption.

Recommendation 5: During any trial of e-balloting for non-statutory balloting, consideration should be given to the use of independent auditors to provide independent assurance for the end-to-end balloting process, including the risk of cyber-attack. It may not be considered practical to utilise external auditors for all industrial action ballots in addition to existing scrutineers. However, it might be thought reasonable to require such assurance for at least industrial disputes affecting 'important public services' as defined in the set of regulations known as the Important Public Services Regulations 2017[1]. Any expectation as to the role of an approved independent auditor could be included in the recommended code of practice.

Recommendation 6: In the event that a trial using e-balloting of non-statutory ballots is agreed, I recommend that the Secretary of State appoints an expert advisory panel whose terms of reference should include:

- Matters for evaluation that are to be part of the trial in addition to those identified in recommendation 3 above;

[1] Important Public Services Regulations, 2017: http://www.legislation.gov.uk/ukdsi/2017/9780111151976/contents.

- The content and process for agreeing a subsequent e-balloting code of practice;

- Reporting back to the Secretary of State.

Recommendation 7: Should e-voting be adopted on a permanent basis, it will be important to retain the option of postal voting to allow the voter choice of channel, not least to ensure that an individual who is more comfortable with postal balloting is not denied that channel.

Recommendation 8: An independent evaluation would need to be carried out if any tests were conducted. It would seem appropriate if the cost of such an evaluation, together with any other test programme delivery costs involved, were met by the Government.

Recommendation 9: If e-balloting for industrial action were approved on a permanent basis the existing code of practice for industrial action ballots should be amended to set the standard that e-ballot coordinators, scrutineers, IT providers, auditors, trade unions and employers should follow in relation to e-ballots. The code of practice should cover the risks of cyber-attack and hacking.

Chapter 1

About the Review/Legal Background

1.1 This review of e-balloting for industrial action was the consequence of parliamentary debate during the passage of the Trade Union Bill[2]. The Government was bringing forward significant reforms to the way that strike ballots were conducted. Trade unions would have to be able to show that there had been a 50 per cent turn-out of those eligible to vote and, where the industrial action had to do with “important public services”, that a total of 40 per cent of those entitled to vote were in favour of action. Those making the case for e-balloting argued that if thresholds were being introduced which had to be met before industrial action was taken it would be reasonable to seek to increase the number of people casting a vote and that e-balloting was one method of doing so. The Government therefore undertook to commission an independent review of the case for electronic balloting for industrial action.

1.2 The position of the Government was that while it had no rooted objection to the principle, it felt that e-balloting presented practical difficulties. For example the balloting had to be secure, accountable and trustworthy enough to retain public confidence. Given that industrial disputes can lead to disruption for the public, the Government was mindful of the need to make sure that any vote in favour of strike action was valid and could not be brought about by outside interference or coercion. The Government was also clear that any new method of deciding whether to take industrial action should be no less secure than the postal ballot arrangements that are currently required.

1.3 The independent review of e-balloting was announced on 3 November 2016. In accordance with its Terms of Reference, the review was required to take into account issues, including but not exclusively:

- The electronic and physical security of e-balloting methods, including risks of interception, impersonation, hacking, fraud or misleading or irregular practices;
- If any system can safeguard against risk of intimidation of union members and protect anonymity of ballot responses;
- The security and resilience of existing practices of balloting of union members;
- The aims of the Trade Union Act 2016 to ensure strikes and related disruption to the public only happen as a result of a clear, positive decision by those entitled to vote.

1.4 The focus of the review was to examine e-balloting for industrial action ballots under the Trade Union and Labour Relations (Consolidation) Act 1992. Accordingly, the review has not considered whether e-balloting is a suitable mechanism to be used for any other type of ballot or any other purpose.

[2] Now the Trade Union Act 2016

1.5 The findings of this review are intended to enable the Secretary of State for Business, Energy and Industrial Strategy, in due course, to make a properly informed and transparent decision concerning whether safe and secure balloting for industrial action can be achieved via electronic processes, and thereafter whether such a system should be permitted across Great Britain.

1.6 I set out the background in a Call for Evidence published on 1 March 2017. The Call for Evidence was due to close on 10 May, however, the announcement of a General Election on 18 April and the pre-election protocol prevented me from publicly promoting the review during the election campaign period. I therefore extended the deadline for responses from 10 May to 14 July 2017. The Call for Evidence resulted in 34 responses through the online survey and individual submissions. The respondents represented a wide range of interested parties, including trade unions, business representatives, individual businesses, academics, technology providers and scrutineers. This report discusses those responses, together with other supporting evidence, and sets out my conclusions and recommendations in the light of my findings.

1.7 Employment law is a devolved matter in Northern Ireland. Accordingly, it will be for the Northern Ireland Executive and the Assembly to determine whether any response on their part is required to the report.

Legal Background

1.8 The Trade Union and Labour Relations (Consolidation) Act 1992 provides that a postal vote is required for ballots and elections, including industrial action ballots, union elections and political fund ballots. However, Section 54 of the Employment Relations Act 2004 contains an order making power allowing the Secretary of State for Business, Energy and Industrial Strategy to widen the methods of voting that are to be used in ballots and elections conducted under the Trade Union and Labour Relations (Consolidation) Act 1992, provided that postal balloting is retained as an option. Nonetheless, the Secretary of State cannot make an order under Section 54 unless he or she is satisfied that the voting process to be adopted in particular ballots meets the 'required standard'. In summary the required standard means ensuring that:

- **All those entitled to vote have an opportunity to do so**;
- **Votes cast are secret**; and
- **The risk of unfairness or malpractice is minimised**.

1.9 Section 4 of the Trade Union Act 2016 makes provision for the Secretary of State to commission an independent review on e-balloting for the purposes of ballots held under section 226 of the Trade Union and Labour Relations (Consolidation) Act 1992. The Secretary of State is required to consider and publish the review and, in due course, lay before each House of Parliament his or her response. For the purpose of preparing that response, the Secretary of State must take soundings from relevant expert organisations and professionals. He or she also has the power to have a test scheme carried out if he or so desires, but they are under no obligation to do so.

Chapter 2

Current ballot processes

2.1 As mentioned in Chapter 1, trade unions are currently required under the Trade Union and Labour Relations (Consolidation) Act 1992 (TULRCA 1992) to hold postal ballots when they wish to call for industrial action, which includes action short of a strike such as an overtime ban. If the required steps are not taken the trade union concerned may be subject to legal action or subject to damages that may be incurred as a result of unlawful action.

2.2 As the Call for Evidence stated, under TULRCA 1992, a ballot paper must be given a unique sequential number and sent in the post to the relevant union members eligible to vote in the ballot. The legislation allows a person eligible to vote the choice of where a postal ballot should be sent - work address or other addresses (such as home). The voting paper must:

- Specify the address to which it is to be returned and the date it should be returned by;

- State the name of the independent scrutineer, where applicable;

- Pose a question which must be asked in a way that can be answered ‘yes’ or ‘no’; and

- In accordance with the Trade Union Act 2016, voting papers will also now need to contain: a summary of the matter or matters at issue in the trade dispute, the type of industrial action proposed and the time period for when the industrial action is expected to take place.

2.3 The response can be sent back in a pre-paid envelope. This process should maintain the voter's anonymity – for example the envelope should not have any distinguishing marks that would reveal the voter's identity. For ballots where there are more than 50 members eligible to vote the union must appoint an independent scrutineer. The scrutineer must then take steps so that they are in a position to make a report about whether the ballot has met all the relevant legal requirements. In addition, the scrutineer must be satisfied that arrangements for the production, storage and distribution of the voting papers included all such security arrangements as were reasonably practicable in order to minimise the risk that any unfairness or malpractice might occur.

2.4 The process must ensure that:

- Everyone entitled to vote is allowed to do so i.e. no-one is accidentally omitted from being asked to vote and that votes are not included from anyone who is not entitled to vote;

- The casting of the vote is done free from interference from, or constraint by, the union or any of its members or employees;

- The votes are fairly and accurately counted; and

- The person entitled to vote should be given an acceptable period of time to vote by post.

SUMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q1. What are the strengths and weaknesses of the current postal system for achieving the required standards?

Twenty nine respondents answered this question. Around a third of their comments referred to the strengths of the current postal system. Around two thirds referred to its weaknesses.

A strong point in favour of postal balloting is its sheer simplicity. There was a significant measure of consensus that the process is clear: trade union members receive their ballot papers in the post (which is generally reliable), they are given reasonable time to make their decision and then, votes having been cast, a tally is made by an independent scrutineer and the result is declared. As the UK Computing Research Committee (UKCRC) commented: "…. it is simple to use: most people are familiar with the process and it requires very little effort to understand how it works."

It can also be argued that other strengths of postal balloting include its accessibility and convenience. While there may be serious issues for some disabled people, which should not be underestimated, the majority of people will have little difficulty with the process involved. Election services provider Sctyl pointed out that the current system meant that voters cast their votes in their own place and time. They added that another advantage was "increased participation", (particularly when voters might not be able to attend a polling station or election site in person e.g. due to absence from the locality, sickness etc).

Whilst not universally welcomed by trade unions when first introduced, the postal ballot has become the accepted way of deciding such matters. Scrutineer, Electoral Reform Services observed that from 1993 postal voting had become a routine and familiar process for trade unions and their members. Members and employers had confidence in the balloting process and were satisfied that the result of voting was an accurate reflection of the views of the relevant group of members. Issues of challenge were usually related to the list of members being balloted, rather than the ballot process itself. Challenges by the employer had usually been related to the accuracy of the information contained in the Notice of Ballot and not the process. They added: "It is our opinion that the current postal balloting system consistently achieves the required standards." Electoral Reform Services also reported that while possible, intimidation rarely occurred under the present system.

However, the volume of negative observations far outweighed the positive ones. I was already conscious of what the Electoral Commission had said in 2014 about the risks involved in individuals voting remotely from the polling station – where, as I said in the Call For Evidence: “people who have been sent postal ballot packs may be more vulnerable to undue influence, intimidation, harassment or pressure to vote in a particular way”.[3] It was therefore not a great surprise to be told in my various meetings about the review that postal balloting was by no means perfect. This sentiment is clearly reflected in the responses.

Intimidation may be relatively rare but there is no doubt that, as a generic method of voting, postal balloting is open to abuse. Thompsons Solicitors Scotland commented: “In relation to the risk of unfairness or malpractice, there is nothing inherent in the current postal arrangements which ensures that the casting of the vote should be done free from interference from, or constraint by, the union or any of its members or employees.” They also remarked that employers frequently ran counter campaigns to dissuade employees from voting to strike or voting at all and pointed out that unfairness, malpractice and voter intimidation were all possible under the postal system, though they reported that they had yet to see any evidence of this occurring.

Voting fraud may be rare under the present system but it is certainly possible and the UK Computing Research Committee pointed to the ease at which postal vote fraud has occurred in non-union ballots, making particular reference to the scale of fraud (nearly half of postal votes cast for the winning candidates) in Birmingham’s 2004 council elections[4]. More recently, some of the many electoral malpractices (including postal voting) that were perpetrated in the London Borough of Tower Hamlets 2014 local elections were subject to scrutiny and exposure through an Election Court and subsequent legal proceedings. Such incidents provide a much wider attack on the integrity of the electoral system and bring a ballot result into disrepute.

The weaknesses of postal voting were pointed out a number of times in my meetings, thus the drawbacks catalogued by the TUC, echoed in a number of other responses, were familiar. The TUC listed the following areas of concern:

- Postal ballots could reduce turnout, particularly amongst younger members and unnecessarily extend the voting period. They did not therefore contribute to the early settlement of disputes and the promotion of good industrial relations;

- Postal ballots were usually more expensive for unions to administer;

- Ballot papers were often misplaced or lost;

[3] The Electoral Commission, Electoral Fraud in the UK: final report and recommendations, January 2014, pg. 13-14.

[4] For more information see ‘Postal voting fraud is 'easy', electoral commissioner says’: http://www.telegraph.co.uk/news/uknews/law-and-order/11560017/Postal-voting-fraud-iseasy-electoral-commissioner-says.html

• Postal correspondence tended to be perceived as junk mail and went into the recycling bin without being opened;

• Individuals could search for and retrieve lost emails, which was not true for paper ballots;

• Reissuing a paper ballot could be time-consuming. Unions had reported instances of members calling union head offices or the ballot agency on the eve of the ballot date reporting lost ballot papers but still wanting to vote. In such cases members missed out on the opportunity of their view being taken into account;

• Members often forgot to provide a change of address;

• Younger members' default communication was often digital, and they tended to change address more regularly, meaning they might be more prone to missing out on postal ballots;

• The fact that unions increasingly communicate electronically meant some members were more likely to inform their union of a change of email address than of their postal address. Whilst unions could make follow-up enquiries where an email 'bounced', they were often unaware if a postal ballot had not reached the right address.

Finally, the cost of postal balloting to the trade unions which, again, was mentioned in my roundtable meetings, is of consideration. It may be indicative that Prospect noted the average cost to it for statutory ballots in the period between 2008 to 2010 was £10,000, the costs associated with sector-wide ballots being "….significantly higher."

Comment

2.5 Postal balloting for industrial action clearly has a number of strengths but it has weaknesses too. It has certainly stood the test of time since its introduction and has been widely accepted as a fair means of reaching important decisions which affect not just the lives of trade union members and their employers, but often the general public too.

2.6 Postal balloting involves a process which both scrutineer and trade union must follow, whereby union members are given a reasonable amount of time in which to make their decision, votes are cast privately, with any irregularities the scrutineer becomes aware of being recorded in their report. This means that all parties, including the employer and the public, where they are affected, know that when action is decided upon the procedures have been properly complied with and a valid outcome has been reached. If the procedures are not followed the employer can seek a High Court injunction to prevent action taking place. Thus a postal ballot is demonstrably fairer and more democratic than the previous show of hands in the works yard or on the shop floor. Everyone knows where they stand under the current process.

2.7 Where a trade union member opts to receive their ballot papers at their home address rather than in the workplace, it is harder to intimidate anyone (regardless of whether it is the trade union, the employer or others who are seeking to intimidate). Likewise, certainly where a large postal ballot involving thousands of workers is concerned, to interfere with the vote as a whole would be a large undertaking.

2.8 It is worth underlining that the postal ballot also offers a period for reflection on the part of the individual trade union member and it can be argued that this is fitting and accords an appropriate respect given the seriousness of the task; i.e. a decision as to whether to take industrial action after careful consideration is clearly preferable to one made in haste.

2.9 I note from the evidence submitted and from the roundtable meetings that one disadvantage of postal balloting is the relatively long duration of the process once all the rules have been followed. Postal balloting can also be costly for the trade unions to implement. This is due to the potentially high postage costs involved, as well the need to provide guidance to trade union officials on the ground, in order that the correct procedures are followed.

2.10 I conclude that while not easy to achieve, coercion and fraud would not be impossible with postal ballots. For example where multiple occupants live in a single dwelling it would be possible for votes to be intercepted by persons other than the intended voter and for abuse, including impersonation and coercion, to occur. Mistakes can occur so that votes are miscast or not cast at all. Authentication is relatively weak, susceptible to error and there is no feedback to the voter or opportunity for verification. Miscounting is possible. In addition, some disabled persons are substantially disadvantaged by postal balloting.

2.11 To this list of drawbacks can be added difficulties reported by respondents such as those caused by delays in the postal system, disruption caused by potential postal service industrial action and the problems experienced by members who work abroad or away from home when votes need to be cast. Nonetheless, while postal balloting may not be perfect it has so far proved to be the best tool we have for achieving the required standard. E-balloting may offer some possibility of improvement, but it brings with it potential risks that need to be understood and mitigated.

2.12 Lastly I understand the view that some reported that the current postal ballot can be subject to abuse and malpractice. However, it is for that reason that in devising an alternative or complementary system via e-balloting there should be careful consideration as to how the scope for malpractice can be eliminated.

Chapter 3

E – balloting processes

3.1 The Call for Evidence made clear that there were different types of electronic balloting, including the provision of digital voting machines for use in polling stations, but that I was focusing on consideration of the use of technology to vote remotely, away from where votes are cast and counted and on a range of systems enabling that. The Call for Evidence noted that there were a number of such systems in use in the UK and that they are used by numerous organisations, not just trade unions.

3.2 The Call for Evidence also discussed the standards required for e-voting. It suggested that the highest standards were needed for general and local elections but that stringent and secure standards of integrity were still needed for balloting for industrial action due to the potentially profound impact a strike can have, not merely on the businesses and employees directly concerned but on wider society too.

SUMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q2. Please give examples of situations where you are aware e-balloting is currently applied. What type of technology is deployed eg. Internet based, telephone based? What has been the impact and how has it been evaluated.

Twenty seven respondents responded to this question. The responses described a range of examples of e-balloting. In just over 80 per cent of cases an internet-based system of e-balloting had been employed.

In my meetings stakeholders were generally keen to give examples of instances where e-balloting was used, both in the UK and elsewhere. The responses to the Call for Evidence were also rich in such examples. One individual noted that there were currently 156 NHS Foundation Trusts in the UK, all of which had to elect governors by consulting their members. Most of these Trusts were trying to move from paper to e-balloting and used scrutineer services. The same individual respondent also indicated that while paper ballots had not been abandoned, some of the UK's building societies used e-balloting for board election purposes, as did a range of sports clubs and associations, housing organisations, (for tenant board elections) and institutions, professional, bodies, charities and political parties (for annual general meetings and board elections), Co-ops (for trustee elections) and Pension Funds (for trustee elections). Other respondents reported similarly.

A range of technology is currently deployed for e-balloting. As outlined above, one of the most familiar uses for e-balloting is to decide building society board elections. Where these are concerned the technology employed is relatively simple: to cast their vote the voter is required to use code numbers received through the post, there is ballot secrecy from third parties and the systems used allow analytical inspection. However, as indicated in the independent report on technology for e-balloting at Annex 4, this kind of e-balloting involves very low level security and it is not at all robust enough to satisfy the 'required standard' for voting on industrial action.

The trade union Unite reported that the Labour Party used both postal and e-balloting when deciding leadership and National Executive Committee posts. Members were encouraged to use e-balloting whereby they used a two part security code to access an online ballot paper and vote. The member could return their ballot paper by post. However, if they voted electronically their paper ballot was invalid. The trade union was unaware of any evaluation regarding this system, but argued that this method of voting would naturally increase participation. No problems were known of the system in comparison to the postal method. In common with a number of other respondents, and as had been said in a number of my meetings, Unite also noted that the Conservative Party had used e-balloting to choose its candidate for the London mayoral election and that, likewise, the Liberal Democrats, the Green Party and the Scottish National Party had also used online voting.

Technology provider Smartmatic listed (not exhaustive) the following countries where internet voting had been used: Estonia, Switzerland and the USA (used at all levels in all three countries), France (general elections), Australia (state/provincial elections) India (state/provincial and local elections), Canada and Chile (local elections in both countries). Denmark also uses internet voting in local elections and industrial action ballots. This respondent argued that the use of internet voting was particularly prevalent in the USA and Canada and that those countries aside, in all the other countries listed "…the scale and size of the populations supported has increased with use over time, and more Governments are seeking to harness online voting as a secure and cost effective channel to engage with citizens." They added that: "With the exception of Canada (which uses internet and telephone voting for local elections), all of the voting approaches utilise a single voting channel, using an internet enabled device (tablet, laptop or smartphone)" and that in Estonia eID was used for access/authentication. The review team visited Estonia to understand how e-balloting worked there and this is reported on in more detail in box 1 below.

Scrutineer Popularis Ltd noted that, in its experience, e-balloting worked best where the employer, union and scrutineer agreed on the procedures for a ballot. In this scenario the employer sent the scrutineer a file of employees names with their current workplace email addresses. The union sent a file to the scrutineer for its members. The data was matched to create a file of union members with current workplace email addresses. Tripartite agreements were made for data confidentiality, firewalls and the use of information during the period of the ballot and the employer agreed to 'whitelist' the scrutineer to allow sending of emails and access to the voting site. Popularis believed that ballots conducted in this way were handled with maximum security and "…ensure that the correct people receive the information on voting and within a defined time to allow swift resolution of the ballot." However, Popularis added "I cannot see that this would work for industrial ballots when co-operation between a union and employer following a breakdown of negotiations on a trade dispute has occurred and emotions will be running high."

Academically robust evaluations of the use of e-balloting are scarce and possibly for the reason that the electoral services provider referred to earlier pointed out: "Independent evaluations of e-balloting do not really take place outside of the organisation that are using the services of scrutineers as each client has their own reason for moving towards it….” However, the Electoral Commission drew attention to its 2007 study of the UK Government’s trial of local authority electronic voting[5]: “We evaluated the pilot schemes, concluding that while the schemes facilitated voting (although they did not have a significant impact on turnout), the level of implementation and security risk involved at the time was significant and unacceptable. There were also concerns about the reliability and cost of e-voting. We concluded that we could not support any further e-voting in the absence of the development by the UK Government of a wider electoral modernisation framework that addressed these issues.”

Additionally, the UK Computing Research Committee noted that Helios voting, the system used to facilitate e-voting by the International Association for Crypytologic Research (www.iac.org) had been subjected to security analyses. This is also true for the system developed by Cybernetica which underlies e-voting in Estonia.

Box 1: E-BALLOTING IN ESTONIA

The review team visited Estonia where internet voting in elections for public office has taken place in eight elections since 2005[6]. Discussions were held with the Estonian Electoral Office and Cybernetica, the company which developed the e-voting software used to administer Estonia’s elections.

In Estonia e-voting supplements traditional methods of voting, such as polling stations or postal voting. Around one in three voters used the internet option in the 2015 parliamentary elections[7]. Similar to Estonian postal voting, a Government issued identity document is used for the internet voting process to ensure the identification of the voter. To protect against coercion, the system allows the voter to revote online, with the new vote superseding the old vote, and arrangements are in place to allow i-voters to vote in the polling station, in which case the internet vote is invalidated[8]. To help ensure voter secrecy, the e-vote is encrypted before the voter’s personal identification is added to the encrypted vote. Once the process has been completed to ensure that only one vote per voter is counted, the voter’s personal information is separated from the internal vote before it is unencrypted to help to ensure secrecy of the data.[9]

The team in Estonia is aware that a 2014 paper from experts at the University of Michigan and the Open Rights Group concluded that “the i-voting system had serious architectural limitations and procedural gaps that potentially jeopardize the integrity of elections”[10]. They were particularly concerned that the system conceived in the early 2000s required that the central servers were trusted to

[5] Electoral Commission, Electoral Pilot Scheme Evaluation, 2007: http://www.electoralcommission.org.uk
[6] Internet Voting in Estonia: http://www.vvk.ee/voting-methods-in-estonia/
[7] Statistics about Internet Voting in Estonia: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics
[8] Internet Voting in Estonia: http://www.vvk.ee/voting-methods-in-estonia/
[9] Internet Voting in Estonia: http://www.vvk.ee/voting-methods-in-estonia/
[10] Drew Springall et al. 2014. Security Analysis of the Estonian Voting System. https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

accurately record votes (the system did not include end-to-end verification), and that procedures to provide security against attack and provide transparency were insufficient. It is noted that the Estonian National Electoral Committee rejected this analysis[11]. An analysis of internet voting in Estonian elections in 2013, 2014 and 2015 concluded that there was no evidence of a "large scale attack on i-voters" being carried out[12].

Comment

3.3 The evidence suggests that there is wide range of situations in which e-balloting has been and is used. The uses to which it is put include deciding general and municipal elections, deciding who is to sit on building society boards, determining who is to take up academic posts and even who is to be given religious office as well as, albeit in cruder form, for deciding the outcome of popular television competitions. In the vast majority of instances, internet voting appears to have been employed.

3.4 However, there have been relatively few evaluations, whether academic or otherwise, of cases in which e-balloting has been used. In the UK the Electoral Commission's key evaluation is ten years old and given the pace at which technology has developed, despite the high level of respect this evaluation is due, one would not wish to place too much reliance on it in view of the context of technology available now. Many 'in-house' evaluations which might be available (and I have received a few such assessments of personal experience from some of those who have used e-voting) are likely to be partial in one direction or the other so, again, one would not wish to overly rely on such reports. It therefore seems reasonable to conclude that before the Government makes any final decision one way or the other about deploying e-balloting for industrial action more research of sufficient rigour is required. In this regard the report commissioned for this review by Professors Ryan and Schneider[13] (Annex 4) is a useful addition to the debate.

[11] Comment on the Article Published in the Guardian, 2014: http://vvk.ee/uudised/vabariigi-valimiskomisjoni-vastulause-the-guardianis-ilmunud-artiklile/

[12] Sven Heiberget al., Log Analysis of Estonian Internet Voting 2013-2015. 2015: https://eprint.iacr.org/2015/1211.pdf

[13] Mark Ryan and Steve Schneider. 26 July 2017: 'Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action'

Chapter 4

All those entitled to vote have an opportunity to do so

4.1 The Call for Evidence noted that this aspect of the required standard of balloting methods - giving access to vote but only to those entitled to do so - represented both an opportunity and a risk for e-balloting.

4.2 Those in favour of e-balloting would argue that if introduced it would drive up turnout, particularly among technically aware young people and, alongside postal balloting, would offer a choice of how to vote as well as ease of access.

4.3 It is possible that electronic voting might offer access benefits, but as the Call for Evidence recorded, any such benefits could be easily undermined if the technology failed to work or was not resilient enough. Technology such as mobile phones and the internet have achieved high penetration levels in the UK but would need to work properly with a range of platforms and systems in order to carry public confidence for a secret ballot.

4.4 The Call for Evidence asked about the benefits and risks of e-balloting in relation to voter access.

SUMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q3. How much do you believe the use of e-balloting for industrial action would increase turnout, if it were available? What other access benefits might it bring?

Twenty nine respondents answered this question. Over 90 per cent believed that e-balloting had the potential to increase turnout, with improved accessibility for disabled voters the most frequently cited benefit.

I was told in a number of my public meetings that e-balloting would drive up participation. Many people seemed to think this would naturally be the case. The feeling also tended to be, particularly among the trade unions, that the general population’s IT skills were now sufficiently developed that e-balloting would present few problems and that in time people would demand it. (Indeed, the evidence suggests that the majority of the working population already has at least some familiarity with information technology). The Office for National Statistics suggests that around 88 per cent of adults and close to 98 per cent of employees accessed the internet in the last three months in 2016, [14] with 82 per cent of adults accessing the

[14] ONS, Internet Access – households and individuals, table 1. 2016: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/datasets/internetaccesshouseholdsandindividualsreferencetables

internet daily or nearly every day[15]). However, there were some respondents who were less sure that turnout levels would automatically increase if e-balloting were deployed.

The response to the first part of the question followed a similar pattern to that which had emerged in the roundtables; i.e. most people (for example the GMB, Prospect, Unite, BMA and the Royal College of Midwives) thought participation would increase, but some doubted it. Unite had no doubt that turnout would rise and argued that: "It simply cannot be the case that turnout will be the same or less than with only postal ballots." Unite underlined that the British Airlines Pilots Association had been using online voting for non-industrial action balloting since 2012 and that it had experienced an increase in turnout of up to 98 per cent and, likewise, that the Communication Workers Union had also experienced a significant rise in turnout. The TUC, the NUSUWT, the Fire Brigades Union and Nautilus all considered that e-balloting had the potential to increase turnout.

Many people I engaged in my roundtables were mindful of younger voters and their expectation that everything in this technology-driven age would be increasingly digitally based. In my view it does seem reasonable to suppose that as more people grow up with IT and the rest of the population adapts to and becomes more familiar with it there is likely to be at least some perplexity if people continue to be faced with paper based voting. This sentiment was reflected in the responses.

The GMB believed that participation would generally increase and that younger members would particularly value being able to vote electronically. Thompsons Solicitors agreed about the likely increase in turnout, "….especially amongst younger workers." Thompsons added "If it can be done from your smartphone or tablet then it requires a minimum of effort at a time which suits you. It seems barely credible that turnout would not increase…."

It is possible that if e-voting were found to increase democratic participation and was seen to do so, a decision to take industrial action, which might otherwise have been viewed as generally unpopular, could actually carry greater support in the public mind. The BMA believed the rise in participation which they anticipated e-balloting would bring about would increase accountability and engagement with the membership, in turn benefiting the public "…as they can be assured that such decisions to take industrial action accurately reflect the considered will of a profession which always has the best interests of patients at heart."

Undoubtedly, a number of unions in the public sector are keen to see e-voting introduced, in part, because they believe it will help them achieve the turnout thresholds introduced under the Trade Union Act 2016 (see Chapter 1). The Royal College of Midwives observed that in 2014/15 it took industrial action for the first time in its history. The ballot was held before the Government introduced turnout

[15] ONS, Internet Access – households and individuals, table 1. 2016: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/datasets/internetaccesshouseholdsandindividualsreferencetables

thresholds. Members in England voted by 82 per cent for strike action but on a 49.4 per cent turnout this would not have been sufficient under the Trade Union Act 2016 to meet the required ballot threshold of 50 per cent. The Royal College believe that if e-balloting had been allowed it was “inconceivable” that it would not have reached a turnout of over 50 per cent.

Some respondents provided evidence that e-balloting would lead to more democratic participation. E-balloting providers, Assembly Voting of Denmark, where e-balloting for industrial action has been practised for some years, reported that at least 11 Danish trade unions used e-balloting, one of them (Dansk Magisterforening) since 2003, and submitted information to suggest that the level of participation had been increased. Smartmatic suggested that e-balloting had increased turnout in Estonia, Switzerland, France, Canada, the USA, Australia, India and Chile. For example, they underlined that according to the post-election report following the 2011 New South Wales State Elections “…usage of iVote greatly exceeded expectations by threefold with almost 50,000 electors using it. We estimate that access to iVote enfranchised around 30,000 electors who were unlikely to vote had iVote not been available.”

However, some other respondents were less positive. More than once in my meetings I was told that that rather than facilitating an increase in voting, e-balloting might simply make it easier for existing voters (i.e. those who would have ordinarily voted by post) to vote but there would remain a ‘hard core’ of people who would not engage.

The Electoral Commission’s response reflected this sentiment. The Commission observed that its evaluation of the UK’s 2007 electronic voting pilots for municipal elections[16] had found that “it was difficult to draw any firm conclusions concerning their impact on turnout. In practice we found that the majority of those who voted electronically were likely to have voted anyway via another channel.” They added that “political science research also suggested that “Internet voting doesn’t generally cause non-voters to vote. Instead, internet voting is mostly used as tool of convenience for individuals who have already decided to vote”.[17]

EEF stated in its response that it was “unconvinced” that e-balloting would help drive up voting numbers. In a meeting with Electoral Reform Services Ltd, their Deputy Chief Executive commented that, in his view, e-voting did not increase participation but was more efficient and made it easier to cast one’s vote. In its response, Electoral Reform Services commented that: “Our experience is that turnout is not linked fundamentally to the type of voting method available to the stakeholder. Engagement with the particular issue being balloted is the prime motivator for participation.” In their response one electoral services provider considered that:

[16] Electoral Pilot Scheme Evaluation, 2007: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0003/16185/ElectoralCommissionOverallReport-Final_27213-20130__E__N__S__W__.pdf

[17] Independent Panel on Internet Voting British Columbia, 2014: http://www.internetvotingpanel.ca/docs/recommendations-report.pdf. pg. 12

"There is no evidence that e-balloting will either increase or decrease turnout of any significance…."

It might ultimately be that the particular issue at stake would determine whether people voted or not (for example, a number of trade unions mentioned in the roundtables how pension rights tend to galvanise their members), in which case the means by which they did so would be irrelevant. There seems much in this point and it is one that was made to me in a number of meetings and it also figures among the TUC's observations.

If e- balloting were introduced it might be that those who might derive the greatest benefit would be those members of the disabled community (perhaps, in particular, the blind[18]) who it was reported are currently disadvantaged by the postal method of voting. A similar outcome was expressed in relation to trade union members who happen to be out of the country when industrial action ballots are held. Box 2 records one disabled trade union member's experience of postal balloting.

Many respondents believed that e-balloting would offer access benefits. For example, a number of respondents, including Thompsons Solicitors, the GMB, Unite, Smartmatic and a provider of electoral services, perceived that there would be improved access benefits for blind people and those with other disabilities. Thompsons remarked that "….access benefits might include benefits for the disabled for whom the use of technology allows them to participate in a way they might not have done before. For example written material needs to be read to the blind and thus impairs the secrecy of the ballot. Technology allows the possibility that adaptive technology already in use will, for the first time, allow for a genuinely secret vote by those groups. Allowing e-balloting would be consistent with the spirit of the public sector equality duty."

Popularis also considered that those who were previously "disenfranchised" ("voters with disabilities, those overseas etc)" would be able to participate more. Scytl was more circumspect and underlined the need to ensure full accessibility to e-ballots for disabled people and the "computer-illiterate". The Electoral Commission was also cautious but did not rule out e-balloting delivering access benefits for disabled people: "E-balloting may have the potential to improve access for disabled trade union members and other hard-to-reach groups. Evidence from the 2007 pilots suggests that it will be essential to engage fully with these groups to ensure that user interfaces are accessible and any potential accessibility benefits are realised."

Box 2: Disabled Trade Union Member, Mr Graham Kirwan

At Unite's request, the review team contacted and spoke to Mr Graham Kirwan, a Unite member who is severely visually impaired, in that he only has peripheral sight. Unite maintained that postal only balloting infringed Mr Kirwan's rights

[18] Viral Voting: Future-proofing UK elections with an #onlinevoting option, 2015: https://webrootsdemocracy.files.wordpress.com/2014/05/webroots-democracy-viral-voting.pdf

(and those of others like him) under Article 11 of the European Court of Human Rights.

Mr Kirwan confirmed Unite's contention that he is unable to vote in trade union (and general and municipal) elections because sufficient adjustments are not made to enable him to do so. Mr Kirwan requires assistance in order to complete paper voting forms and the level of assistance needed is such as to infringe the secrecy of the ballot.

Mr Kirwan also confirmed that he had only ever been able to vote independently in recent Labour party elections where he was able to access the relevant online system and vote using software which magnified the voting information (and process) on his computer screen. Thus Mr Kirwan argued that he was excluded from participation in industrial action ballots and that if e-balloting technology such as that used by the Labour Party were deployed he would be able to participate fully.

Comment

4.5 It is difficult to draw any firm conclusion as to whether e-balloting would increase turnout because the evidence is so mixed. Undoubtedly it would be in the interest of democracy if participation were to rise. It would also be of potential benefit to the public, in that they might more easily be reconciled to a public sector strike. There might also be benefit to the trade unions themselves, in that they might be perceived in the minds of some of their members as more relevant, which might prompt increased engagement. I conclude that turnout is something to look at in any e-balloting trial that might be undertaken.

4.6 Where access is concerned, I see no reason to disagree with those who contend that among those who would benefit from e-balloting would be some disabled voters and those such as sea faring trade union members who might be overseas when a vote was called on industrial action by their union. The ease at which one might vote using a hand-held device such as a smartphone or tablet would, on the face of it make it more likely that someone would be motivated to vote and that their vote might be received in time to make a difference. Again, however, this is something which could very usefully be examined under the test of e-balloting technology which I believe is merited. If there were such a test it would be important to examine the accessibility of any system for disabled people and others with special needs.

SUMMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q4. Which forms of e-balloting system (e.g. telephone, internet) would help ensure access? What evaluations have taken place on the robustness and resilience of different systems to ensure access in a voting context?

Twenty nine respondents answered this question. Approximately 80 per cent considered that an internet-based system of e-balloting would help to ensure access.

As mentioned in Chapter 3, rather than focusing on digital voting machines for use in polling stations I have concentrated on methods of voting remotely. There is a range of technology on the market to this end. A number of respondents did not rule out the use of telephone voting. However, for a ballot concerning something as crucially important as whether or not to take industrial action the use of a traditional PSTN (Public Switched Telephone Network) would seem inappropriate. One individual respondent said: “There is very little use of telephone voting, it is offered and I cannot think of the last time anyone ever asked for it other than RNIB (Royal National Institute of Blind People), who use ERS (Electoral Reform Services) currently as a scrutineer. Generic telephone companies are used to collect telephone votes using scripts and tone responses. Telephone systems are deemed to be the most insecure method of voting, due to authentication, use of a non-secure channel and system being outside of direct scrutineer control (i.e. using independent telephone company).” Smartmatic noted that: “…there has been little innovation in the realm of telephony and many of the modern cyber-security measures and techniques which we see in the online world, cannot be applied to telephone-based systems, rendering them far less secure than online systems.”

The e-balloting research commissioned from Professors Ryan and Schneider[19] looked specifically at four remote electronic balloting systems: that which is used for building society elections; Helios (an open source online voting system); Cybernetica’s online and mobile phone enabled system used in Estonia; and CH Vote, an internet system used in Switzerland.

All four systems detailed in the research that was commissioned were weighed against postal balloting and each had relative drawbacks as well as strengths. For example, while one might be encouraged by the accessibility of the technology used to conduct building society elections it fails the security test, such as the detectability of cyber-attack, which results in the integrity of the vote not being guaranteed. This would make the technology unsuitable for use in determining something as serious as a trade union industrial action ballot. Helios, the Estonian system, and CHVote are considered to be more secure in terms of cyber-attack but have other weaknesses, such as around potential coercion from a third party. While the current Estonian system is perhaps the most secure (although it is not perfect) it is not as accessible as it might be as it relies on the Estonian Digital ID card which all Estonian citizens are issued with. (Alternatively the citizen can use a smart card containing their eID).

Leaving aside any other security concerns, whether the Estonian system could work in the UK using a different form of personal access, e.g. a two part PIN code, would need to be tested. As was said more than once in my roundtables, Government should avoid making the cost or difficulty of accessing e-balloting systems such that the user is effectively barred or frustrated, and I am mindful of the need for the cost to be no more than appropriate: the cost of the technology should be no more than necessary to cover the security which is needed.

[19] Mark Ryan and Steve Schneider. 26 July 2017: ‘Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action’

As indicated in the summary of evidence under question 3, the needs of disabled people and general ease of accessibility would be a key consideration in the design of any e-balloting systems that might be employed. The Electoral Commission noted that its evaluation of internet and telephone voting systems used in the Government's 2002-2007 pilot programme underlined the importance of this point. The TUC observed that Scope, a charity for people with disabilities, reported its findings from the aforementioned Government pilot in its 2010 Polls Apart report on opening elections to disabled people.[20] They considered that: "many disabled people who piloted [online voting] were pleased that for the first time they were able to vote independently, without assistance" although navigating between voting screens was confusing for some. Scope recommended that: "The Electoral Commission and the Government should trial accessible e-voting solutions for blind and partially sighted people such as telephone, text and online voting as well as handheld devices."

The TUC pointed out that younger union members would benefit greatly from e-balloting being introduced, a point covered already in the evidence under question 3.

If e-balloting were trialled for non-statutory ballots it would be helpful if it could run in parallel with the postal ballot alternative. The UK Computing Research Committee (UKCRC) considered that if the two systems were to run in parallel it would be necessary to examine what this might mean for security. In doing so UKCRC stated: "… it could be the case that the resulting hybrid system may not retain the same security properties as its two constituent sub-systems."

Where systems are concerned, given the speed of innovation and change in the IT sector, to avoid building in obsolescence and leave scope for development it would be important for the Government to avoid taking a prescriptive approach; the more open the approach the better. This sentiment was heard a number of times in the discussions. In particular the Employment Lawyers Association believed it would be best to be as open minded as possible in the approach: "A combination of methods would be preferable in terms of achieving optimum access for voters. Utilising different forms of e-balloting such as telephone, internet, App and voting machines, should ensure wide catchment and inclusion regardless of disability or differing socio-economic circumstances."

Putting aside how the means of identification might be sent to the voter and how it would be in two parts etc, it would seem reasonable to suppose that, for the average voter, among the benefits of e-balloting via the internet would be the ease and convenience of having all the relevant information in one place.

[20] Polls Apart 2010: Opening elections to disabled people: http://www.scope.org.uk/Scope/media/Documents/Publication%20Directory/Polls-apart-2010.pdf

Comment

4.7 I conclude that it is sensible if there is to be any subsequent trial to confine the assessment of e-balloting to voting using the internet as accessed by smartphone, computers and the internet. Equally, there is little value in considering the use of telephone voting; the lack of security involved precludes this means of voting from further consideration.

4.8 In providing e-balloting the challenge is giving access to the right people (those entitled to vote, and *only* those entitled to vote) ensuring secrecy of a ballot and providing sufficient ease of access without making it either so easy to vote that anyone can vote or over-engineering systems such that the expense of providing a secure system becomes difficult to justify.

4.9 A number of unions have said they should be left to decide with the scrutineer the means of voting to be used for a given industrial action ballot. It is correct that the trade union will know its members best and how they might best be engaged. Therefore a trade union could discuss the means via which a vote might be held, choosing between internet voting and postal balloting or postal voting only. Under any trial which might be held following this report the two methods would be on offer anyway. The trade union might also advise on how its members might best access the vote (eg by smartphone, computer etc). However, trade unions should only be able to choose electoral service providers/scrutineers from a list approved by the Secretary of State. In view of the need for effective security I would not suggest that it should be open to all to establish an e-balloting service without such Government approval. Any e-balloting system which is designed will need to factor in the requirements of disabled people, older workers and those with learning needs. Moreover, any subsequently agreed trial should consider whether the parallel running of postal balloting and e-voting raises fresh security challenges and, if so, how these might be deal with.

Chapter 5

Votes cast are secret

5.1 In the Call for Evidence I talked about the need to ensure anonymity in an industrial action ballot being no less important than for a general election. I also noted that voter coercion was the main threat to be guarded against for most voting systems.

5.2 At present trade union action ballots are conducted away from the workplace, often at home and generally, in private. I was interested to know whether a switch to remote electronic balloting, meaning many union members were likely to vote on smartphones in response to emails, might alter the current private voting dynamics. That is, a smartphone might be taken to the workplace, and I questioned if this might compromise the integrity of the vote by offering a greater risk of coercion.

5.3 I also wanted to know what the implications of e-balloting technology would mean where voter secrecy was concerned: for example whether it might be possible to hack an e-balloting system and discover how someone had voted, or whether e-balloting actually be an improvement on postal voting and mitigate voter coercion.

SUMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q5. In what circumstances might e-balloting be more or less secret when compared to postal voting?

Twenty nine respondents answered this question. Just under 60 per cent did not envisage that e-balloting would alter the secrecy of voting. Nearly 17 per cent believed that e-balloting could improve secrecy, while 10 per cent considered that it might reduce levels of secrecy.

Despite the misgivings about postal balloting which the Electoral Commission referred to in its 2007 study of the UK Government’s trial of local authority electronic voting, no one I spoke to or who submitted evidence suggested that there were any security problems with it where it was used by the unions to decide on industrial action. Therefore, while we know that problems can and do occur in general and municipal elections, it would seem to be a misrepresentation to suggest that postal balloting is not working effectively for trade union ballots, and the scrutineers did not suggest there was evidence of abuse.

Nonetheless, it was pointed out that postal balloting could be the subject of malpractice; a number of respondents accepted that postal balloting and e-balloting both carried potential risks regarding secrecy and cohesion.

However, some respondents believed that e-balloting was superior to postal balloting where secrecy was concerned. Smartmatic observed that: “It is our unwavering belief that a well-designed e-balloting system is overwhelmingly more secure than postal voting.” Smartmatic underlined that, unlike e-balloting in their view, postal balloting was susceptible to fraud (interception/impersonation) and coercion. Scytl argued similarly. Some would no doubt argue that should e-balloting be proven to fulfil all the secrecy requirements that might reasonably be demanded, it should be judged as capable of maintaining secrecy to a potentially greater extent than the postal method. As Scytl argued: “Advanced cryptographic protocols existing nowadays can provide end-to-end privacy, integrity and verifiability to voters, auditors and election officials.”

As indicated above, the traditional postal process can be interfered with at all points; integrity is at risk whether through impersonation, during transit of the voting papers, or during the count/announcing the result. Those in favour of e-balloting argue that, unlike postal balloting, e-balloting is capable of ‘end-to-end’ verification (by the individual voter and/or an independent observer) meaning that a voter can check that their vote remained as cast in the declared result, that only those who should have voted did actually vote and that the declared result is the correct one.

Electoral Reform Services (ERS) considered what is required to ensure secrecy for e-balloting in their 2015 report:[21] “It is good practice to separate, physically and electronically, the system and data base 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 the two systems is the authentication code. This ensures that the voter’s identity is separated from their voting preference but, as currently with public elections and other postal ballots this allows, in the event of subsequent challenges, for the independent person to investigate and if need be invalidate the votes from a particular voter. It may be appropriate for the data related to the ballot to be encrypted when stored to further enhance the security and secrecy of the vote.”

ERS found in their 2015 report that e-balloting is neither more nor less safe than postal balloting. Both methods have their risks. As the ERS said: “Many of the issues relating to casting an electronic vote in secret are similar to those when completing and returning a postal ballot paper….specifically in relation to secrecy voters should consider their physical location when they cast their vote and the proximity of others to them.”

Just as postal balloting has its drawbacks, it can equally be argued that the secrecy and integrity of e-balloting can also be compromised. For example, Popularis noted that it was not possible to tell when sending information in an email whether the information had not been automatically forwarded to someone.

In the roundtable meetings, and to some extent in the responses to the Call for Evidence, there was a difference of opinion as to whether or not the employer’s IT system should be used to conduct e-ballots. For example, a number of trade unions were relaxed about this but others were not. The NUT observed: “For those voting online at work there may be a risk of the employer monitoring their online activities and technology is likely to be in place to find out when the worker has voted, the technology may also mean that the employer can find out how the worker has voted.”

[21] Trade Unions and E-Voting, is it possible?: https://www.electoralreform.co.uk/trade-unions-and-e-voting-is-it-possible

Jaguar Land Rover made a practical point at one of the roundtables which was that by no means all of its employees had access to a computer at work, so it would not be possible to ballot all union members in any particular plant using the firm's IT. No doubt other employers may be in a similar position, but of course postal balloting would still be available.

In weighing the relative potential of postal balloting and e-balloting to safeguard secrecy, the UKRC was able to identify advantages e-balloting presented. These were that: (i) "there might be special mechanisms that could be engineered into the system to allow a level of coercion resistance"; and (ii) that "with cryptographic techniques allowed one can facilitate the electronic counting of votes in a collective way at a mass scale … This allows for processing the votes in the largest possible sets, thus increasing anonymity in terms of the size of voter pool".

EEF took the view that in order to justify its introduction, e-balloting would have to be able to outperform postal balloting on secrecy. They contended: "Electronic balloting would need to provide greater levels of secrecy than a postal ballot in order to promote confidence in the platform."

Comment

5.4 In order to carry confidence, e-balloting has to stand on its own merits and be seen to be as secure as postal balloting. What is needed is a level of security which is proportionate and fit for purpose.

5.5 While there are risks in common with those experienced with postal balloting, e-balloting introduces some different challenges relating to secrecy. It may be that overtime the assertions of those who argue that e-balloting is superior to the postal method in terms of protecting secrecy will prove justified, but only stringent testing will reveal this. Specifically, such testing will also reveal whether the technology is capable of providing the end-to-end verification which is needed in order to give trade unions, their members, employers and the public the confidence they would need if e-balloting is to ever be permanently deployed as an alternative voting system.

5.6 I indicated in my Call for Evidence that for the purposes of this review I intended to "…focus on considering an approach that uses technology to allow someone to cast a vote remotely (i.e. somewhere separate from where any other votes are being cast or counted". However, as noted above, a number of respondents raised whether it should be possible to use a workplace IT account to take part in an electronic ballot. I have considered this issue. On the one hand, it could be argued that if the Government were to allow this it would be a return to voting in the workplace and that intimidation might increase. On the other hand, leaving aside for a moment the possibility of intimidation and whether trade unionists would wish to reveal to their employers that they were union members, it might be argued that if an employer were willing to let their system be used for a ballot it should be allowed. That said, I note Popularis' comment (see page 15) about whether it is a realistic possibility that in a situation where feelings on both sides are running high an employer would be willing to facilitate a ballot by allowing their IT system to be used.

5.7 It strikes me that the use of workplace IT systems might usefully be explored, but I leave it to the Secretary of State to consider whether it is appropriate to allow in any e-balloting test. Nonetheless, I would observe that postal balloting will clearly remain an option whether or not workplace IT systems are used, so their use is not essential. In my view, if workplace IT accounts were deployed in any test there should be no obligation on the employer to assist (in lifting firewalls etc) if they do not wish to.

SUMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q6. What mitigations can be employed to ensure that under e-balloting, hacking of the system, even if successful, would not allow the identity of a vote to be revealed? Have such mitigations been evaluated?

Twenty seven respondents answered this question. A wide range of mitigating solutions was suggested, including ensuring that an independent scrutineer conducted the ballot and using encryption security methods to protect the vote.

There is little doubt that forces exist which may be tempted to interfere with general elections, for example it was recently reported that Mart Helme, Chairman of Estonia's EKRE party, had claimed that it was possible that a foreign power had set its sights on Estonia's October 2017 local elections. In my roundtables I discussed whether any nation state would be motivated to hack into an information technology system supporting an e-ballot for industrial action. Many trade unionists (and one or two others) argued that this was not a credible threat or was at most extremely unlikely, it being simply not worth the trouble given the relative unimportance of such ballots. Popularis contended that it was unlikely to be worth the effort of trying to hack into its systems and that it would be easier to penetrate the email sent to voters containing the information they would need to vote.

A minority of other respondents disagreed and thought it entirely possible that either an ill-intentioned nation state or someone seeking to cause as much trouble as possible - simply for the challenge presented and because they had the IT skills to do so - would be motivated to hack into such a vote or to develop malware designed to interfere with the means of voting (smartphones, laptops and mobiles and servers). The report I commissioned from Professors Ryan and Schneider[22] takes the threat of hacking seriously. The authors noted in relation to industrial balloting that a variety of people would be interested in interfering: "Such people can include the directly related parties (employers and employees), or politicians, journalists or other kinds of commentator and observers. They can also include organised criminals and possibly state-sponsored agents, that may be interested in industrial sabotage or damaging the economic well-being of the country."

One of the first requirements if e-balloting were to be trialled (and in any subsequent roll out) for industrial action ballots would be to appoint a scrutineer, an independent party who, as with postal balloting, would check that voting had taken place properly

[22] Mark Ryan and Steve Schneider. 26 July 2017: 'Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action'

and that the result was correct. The scrutineer could also (although not necessarily) be the provider of the electronic system used for voting. An electoral services provider underlined in their response that all statutory elections around the globe always employed a "… third party auditor to confirm the system being used for security purposes."

There is a reasonably well-trodden path to be followed to put together an e-balloting system. The ERS set out in its 2015 report 'Trade Unions and e-voting-is it possible'[23] the steps that one should take. These include: authenticating the voter's identity; ensuring that third parties are not able to capture or interfere with distribution of the ballot information; maintaining the integrity and security of the ballot by using secure methods to distribute the ballot information; and minimising the risk of unfairness or malpractice.

In its specific response ERS itself said: "When conducting a postal voting project it is good practice to ensure that there is separation between the list of voters that may also contain the allocated voting paper number and the voting papers. This separation of information minimises the risk that an individual's vote will not remain secret but also, if required, enables investigation of the voting process. This mirrors the processes used at public elections in polling stations or postal vote issuing. An e-balloting system should also use this principle of separation of data to minimise the risk that the identity of a vote could be revealed."

Different organisations and countries have designed e-balloting systems in different ways and with varying degrees of success. The UK Computing Research Committee set out what can be done in their response: "in particular, advanced encryption measures such as homomorphic encryption have been demonstrated to be very useful in preserving the privacy of encrypted ballots while enabling the computation of the final tally. Another technique that has been successfully employed in the context of e-voting for anonymisation of the submitted ballots is the use of a mix-net which is the electronic equivalent of shaking up the ballot box to mix up the votes, so no cast vote can be associated with any individual. In terms of coercion, a number of techniques have been proposed to reduce the opportunity for coercion/intimidation in the context of e-voting, for example by allowing re-voting to overwrite an earlier vote or issuing voting credentials that do not contribute to the final tally (and may be shared with a coercer). There has also been work on automatically identifying ballots that were cast as a result of coercion, and removing them. Using cryptographic mechanisms properly, the level of vote secrecy provided by e-balloting can be reasonably high, at least in theory."

A vote on a matter as important as when to take industrial action demands that the balloting system should be as robust as possible. The mitigating steps employed in Estonia were explained to us by Cybernetica when the review team visited them and at first face these appear to be at the level which seems to be needed. Cybernetica's

[23] https://www.electoralreform.co.uk/trade-unions-and-e-voting-is-it-possible

system has been evaluated, for example in the report E-Voting in Estonia.[24] The technological report commissioned from Professors Ryan and Schneider (see Annex 4) assesses a number of systems which have been used for e-balloting, including the Cybernetica system used in Estonia. Among the measures taken against hacking in Estonia are the encryption of the vote using a public and a secret key so that it remains secret to the point of decryption for counting to take place. In addition only the last vote cast by the voter counts; and a cryptographic mixnet is used to anonymise the encrypted votes received. (For full details see Box 1 on pages 16-17).

For its part, Usdaw underlined that it only conducted industrial action ballots after a lengthy consultation process and that during the ballot period it was in constant close touch with members to be aware of the mood. Therefore in Usdaw's view: "In the highly unlikely event of any cyber-attack, the Union would recognise a result that is not expected."

Comment

5.8 E-balloting has for some time been used successfully in a number of countries. For example, Estonia has been conducting local elections electronically since 2005 and general elections since 2007. Likewise, Denmark has been using e-voting for industrial action ballots for over ten years.

5.9 Nevertheless, while carrying out this review I have been struck by how often cyber security issues have figured in current affairs and by how vulnerable to attack public and private sector information technology systems appear to be. For example, in April 2017 it was reported that the Foreign Office had come under a sustained cyber-attack from a group of hackers alleged to be linked to a foreign state. The perpetrators were said to have tried to infect Foreign Office systems with malware and that the Government reported that it faced tens of thousands of cyber-attacks every month.[25]

5.10 I understand that before this year's general election, UK political parties received a security briefing concerning possible hacking of digital systems following reports of Russian interference in the 2016 US presidential elections.[26] Since then it has been alleged that Russian intelligence agents hacked a US company supplying electronic voting services and equipment in the weeks preceding the 2016 US presidential elections and attempted to affect vote counting via malicious emails.[27] It has also been reported that the 30 July 2017 electronic ballot for Venezuela's constituent assembly was manipulated.[28] Internet voting may also be compromised by technical issues. In Geneva the addition of a Java applet to the city's internet voting application resulted in compatibility issues, limiting the number of platforms on which the app could run and

[24] Nikhel Solvak & Kristjan Vassil, E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015), 2016: https://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil_solvak_a5_web.pdf

[25] 'Foreign Office hit by 'Russia hackers'. The Times. 14th April, 2017.

[26] 'Parties on alert for hacking threat'. The Times. 22nd April, 2017

[27] https://www.theguardian.com/technology/2017/jun/05/russia-us-election-hack-voting-system-nsa-report

[28] 'Venezuela poll was rigged, says voting company'. Financial Times. 2 August, 2017.https://www.ft.com/content/2df422b8-779d-11e7-90c0-90a9d1bc9691

reducing voter turn-out by an estimated 3-4 points.[29] In May 2017 the WannaCry cyber-attack occurred and the world's computer systems were held to ransom. This attack caused the shutdown of many NHS hospitals in Britain and disrupted rail networks in Germany, telecommunications in Spain and banking in China.

5.11 In January 2017 it was said that cybercriminals were charging a mere £20 to cripple websites.[30] This could be achieved relatively simply by the use of 'botnet' armies which overloaded websites with data. It was alleged that it was possible to tour hidden websites and contract with criminals for illegal services such as altering examination grades by interfering with universities' administrative systems.[31] In May 2017 it was reported that 5.5 million people in the UK alone had been obliged to cancel their credit or debit card because of unprecedented levels of cyber-attacks[32] and in June hackers forced the parliamentary authorities to close remote access to email accounts used by MPs, peers and researchers.

5.12 Even more relevant to this report was a warning from the former head of MI6 in January 2017, that electronic voting could be vulnerable to cyber-attack: He said: "The more things that go online, the more susceptible you are to cyber-attacks." He added: "Bizarrely the stubby pencil and piece of paper that you put your cross on in the ballot box is actually much more secure than anything which is electronic."[33]

5.13 There is little doubt that there is a scale of importance where ballots are concerned, on a spectrum ranging from a television competition to the democratic decisions of local and general elections. As already indicated, I consider that a trade union industrial action ballot may not be at the democratic election end of the polling spectrum, however it is not far from it.

5.14 It appears to me that there is a real threat of malevolent attack on Britain's IT systems, whether from criminals, those seeking to frustrate users or from those directly or indirectly employed by ill-intentioned foreign states. In my view it is not impossible that such people would be motivated to disrupt and interfere with a trade union ballot for an industrial dispute. The consequences arising from disruption in either the public or private sector could inflict real damage to the country.

5.15 A trade union industrial action ballot is a very serious matter and particularly so where the result is connected to one of the "important public services". The amendments made by the Trade Union Act 2016 enabled the Secretary of State to make regulations to specify the "important public services" captured by the 40% threshold. Such a vote is not only important to the trade union, the trade union member and the employer but is also vitally important to the public. It is not fanciful to believe that those who wish to cause disruption to a legitimate ballot result might try to do so if the security protocols

[29] Michel Chevallier, 2009: 'Internet Voting, Turnout and Deliberation: A Study

[30] 'Cybercriminals charge just £20 to paralyse websites'. The Times. 11th January, 2017

[31] 'Cybercriminals charge just £20 to paralyse websites'. The Times. 11th January, 2017

[32] 'Cyberattacks force millions to cancel bank cards'. The Times. 23rd May, 2017

[33] Former MI6 chief warns against introducing electronic voting, 2017: https://www.politicshome.com/news/uk/political-parties/labour-party/news/82041/former-mi6-chief-warns-against-introducing

are not robust. It will be important to conduct a test programme before e-balloting is ever implemented and to do so over a ‘reasonable’ period of time. If there is a decision to proceed, the Secretary of State should decide what a reasonable period of time is and any test programme should be followed by a full evaluation which the Secretary of State should consider in detail before deciding on next steps.

Q7. Would e-balloting increase the scope for intimidation and undue influence (being forced to vote, and being forced to show which way someone had voted, and being forced to vote in a certain way)?

Thirty one respondents answered this question. Around two thirds of respondents did not consider that e-balloting would increase or decrease the potential for voter intimidation and coercion. One third believed that e-balloting would reduce the scope for such behavior.

It is worth reflecting on the legal requirements regarding interference/intimidation: The Trade Union and Labour relations (Consolidation) Act 1992 (as amended) states that: “Every person who is entitled to vote in the ballot must:

“be allowed to vote without interference from, or constraint imposed by, the union or any of its members, officials or employees” Section 230(1)(a) and

“the scrutineer’s report on the ballot shall state whether the scrutineer is satisfied - that there are no reasonable grounds for believing that there was any contravention of a requirement imposed by or under any enactment in relation to the ballot.” Section 231B(1)(a).

It can be seen that the legislation sets the bar at a relatively high level where intimidation and undue influence is concerned. While the Electoral Commission pointed out in its response that any balloting system away from a polling system could be open to improper pressure and influence being exerted on the voter, Electoral Reform Services (ERS) commented: “In our experience as a scrutineer since 1993 we have not had to deal with a complaint from a member that alleges intimidation or undue influence that has required us to qualify our independent Scrutineer’s report.” Accordingly, whilst there is a potential risk of abuse, it does appear that the current postal system of balloting seems to work in regard to interference and undue intimidation. Indeed no one has complained to me during this review about such practices.

The introduction of the secret postal ballot for industrial action replaced a public show of hands at a workplace to decide matters, giving much more protection for trade unions member against intimidation. In deciding whether to deploy e-balloting it would be important to ensure that it was not a retrograde step that weakened the integrity of the vote: as the Local Government Association observed: “….if electronic balloting is put in place, sufficient safeguards should also be put in place so as to ensure voting systems remain secure and the risk of unfairness and malpractice is minimised.”

Some respondents believe e-balloting would take balloting backwards. For example, an employer group said: "….if voting in an electronic ballot could take place by use of hand held devices there may also be potential claims of trade union intimidation." In addition, one individual commented: "My long but now historic experience of trade union activity leading up to strike balloting makes me sceptical regarding the claims made by supporters of e-balloting. Coercion coupled with personal threats to members and their families has long been a weapon used by militants attached to the Trade Union movement." The trade unions generally argued in their responses that e-balloting would not increase the scope for intimidation or undue influence in industrial action ballots. They asserted their right to legitimately influence how members voted, perhaps by recommending choices and argued that this was not at all the same as intimidation.

A practical way of making sure that any intimidation which did occur was neutralised would be if 're-voting' (or multiple voting) were allowed (as in Estonia). In such arrangements a voter would be able to vote electronically as many times as they liked but only the last vote would count. Smartmatic recommended re-voting and questioned why one would wish to deny oneself a benefit offered by e-balloting simply because it was not available under the traditional approach. Other respondents agreed. It was also pointed out that the opportunity to re-vote also provided a period of reflection during the time the opportunity to vote remained available.

However, others were not at all positive about re-voting. One individual cautioned: "Any surrender of the current disciplines which apply to secret postal balloting do need in my view to be weighed carefully by the risks that e-balloting may open up abuse in ways which are difficult to necessarily envisage in advance." And ERS said: "we would caution against allowing re-voting when there is no evidence that [it] is required and it cannot be easily or practically replicated in a postal process." ERS underlined that where a scrutineer was required to monitor and then report on any intimidation or undue influence a revote was unnecessary.

If e-balloting were trialled alongside postal balloting and should re-voting be part of the process for evaluation one would need to consider the UK Computing Research Committee's observation that: "…re-voting may introduce other complications in the verification of the tally that need to be carefully evaluated before deployment." With regard to combining incoercible e-voting systems (systems where it is not feasible to coerce the voter to vote a particular way) the Committee also suggested further research was needed.

Comment

5.16 All balloting systems are potentially open to abuse. Such interference is very difficult to stop, being both hard to identify and to prove. We have seen evidence of such abuse in local democratic elections, albeit rarely.

5.17 Likewise, it would be possible to attempt to intimidate and unduly influence the outcome of a ballot for an industrial dispute under the existing arrangements. That said, as noted earlier, it would be very difficult to organise abuse on a wholesale basis for a large postal ballot, given the need for intimidation/undue influence to be carried out individually.

5.18 Along with the relevant penalties, the fact that each ballot is monitored for abuse may in itself act as a deterrent for some potential wrong doers. The prevention of abuse principally relies on reports of infringements from interested parties; i.e. employees, trade unions and employers. Scrutineers are rarely required to report instances of wrong doing, so it would seem that either the sanctity of the ballot is being respected or abuse is going on ‘underneath the radar’ and has not been detected.

5.19 The integrity of the vote is of paramount importance. If e-balloting is introduced it would be essential that it was no more susceptible to abuse than postal balloting. A trial should test and evaluate whether it is possible to fulfil this requirement. In this regard, re-voting could be trialled, both to see whether it could work and what the reaction/perception of trade union members was to the re-vote facility. One could also look at the potential of incoercible e-voting systems.

Chapter 6

The risk of unfairness or malpractice is minimised

6.1 The Call for Evidence flagged that there were a number of issues to be considered under this heading which required a technological response when e-balloting was deployed, namely:

- the need for voter verification;
- the risk of interception or interference;
- the possible need for greater functionality than with postal balloting, for example the need for voter verification that the vote has been recorded as cast and the scrutineer to verify that recorded votes had been accurately counted.

6.2 The Call for Evidence noted that some people expressed concern as to whether the technology could deal with these challenges at present. The Open Rights Group was quoted as saying "Voting is a uniquely difficult question for computer science: the system must verify your eligibility to vote; know whether you have already voted; and allow for audits and recounts. Yet it must always preserve your anonymity and privacy. Currently, there are no practical solutions to this highly complex problem and existing systems are unacceptably flawed"[34]. However, the Speaker's Commission, cited in the above Open Rights Group report, concluded that: "It is only a matter of time before online voting is a reality, but first the concerns about security must be overcome."

SUMMARY OF RESPONSES TO THE CALL FOR EVIDENCE

Q8. How do you believe technology has evolved or will evolve to address the risks set out above?

Twenty six respondents answered this question. A total of eighteen suggestions were made for how technology might address security risks.

No one queried the issues raised in the Call For Evidence's question and the CWU (Communication Workers Union) observed that: "The challenges identified by the call for evidence include voter verification and ensuring security from interception and interference. The CWU agrees that these are the main issues to be addressed."

It is in the nature of technology that it evolves and at pace. Unfortunately so do the cyber threats that confront it and a number of respondents have underlined this point, including Popularis and the TUC. Electoral Reform Services (ERS) neatly summed up the situation in saying: "Internet security can seem like an "arms race" between developers and hackers, every time a developer fixes a bug or vulnerability, some

[34] Open Up! Report of the Speaker's Commission on Digital Democracy, 2015: www.digitaldemocracy.parliament.uk/documents/Open-Up-Digital-Democracy-Report.pdf

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."

A common theme among trade union respondents, and something which surfaced in my roundtables involving them, was the emphasis on the need to avoid being overly prescriptive about how online IT systems should work in order that the systems can keep up with technological developments. WebRoots also identified this concern and said: "It would therefore be unwise to specify in legislation a fixed process or digital infrastructure for trade unions to use for an online voting system. Any online balloting system that is introduced should have the scope to be fluid, regularly updated, and strengthened in order to effectively combat the cyber-security challenges of the future." Unite counselled that any laws allowing e-balloting should be: "…flexible, referring to required standards rather than mechanism."

If e-balloting is to be tested it would be very useful to be able to have some idea of the current and upcoming issues in e-balloting system design. Smartmatic has attempted to provide some. They raised the following:

- Digital identity – Using digital platforms including biometric information to ensure eligibility and eliminate identity theft and impersonation;

- Information security and cryptography – Developing new systems and technologies to protect electronic messages and data from 'eavesdropping' and/or tampering; and

- Verifiability and provable security – Delivering tools which irrefutably prove the integrity of electronic messages and data in a provable and transparent manner (such as using 'blockchain' technologies).

The UK Computing Research Committee (UKCRC) advised that: "From a general security perspective, upcoming and currently ongoing developments (e.g. the development of secure communications protocol TLS1.3) are expected to improve the security of internet connected devices which can be directly beneficial for the E-balloting case."

The technological challenge of e-voting is highlighted by a recent security threat to the Estonian ID cards that are used for e-balloting.[35]

As indicated above, while much effort is continually going into internet security issues those wishing to interrupt IT systems do not stand still either. For this reason no doubt, the UKCRC also observed: "Despite successful adoption of e-voting systems in a number of instances there still appears to be no e-balloting system that solves all conceivable problems and there have been a number of concerns voiced against the use of e-balloting in national elections." However, they cautioned that the fair comparator for e-voting was postal balloting, which had itself encountered attacks on its integrity.

[35] Red faces in Estonia over ID card security flaw: https://www.ft.com/content/874359dc-925b-11e7-a9e6-11d2f0ebb7f0

There is a demand to ‘get on’ with e-balloting and this came through in the roundtables and in some of the responses. Many trade unions would like to proceed to e-balloting now. In addition, some IT providers will argue that their technology is already fit for purpose. For example, while recognising that matters would keep evolving, Scytl said: “the technology has evolved to the extent that e-balloting can be considered a highly secure voting channel, surpassing traditional paper based and postal voting in several aspects.” For its part, ERS commented: “We cannot see why the introduction of e-balloting would require changes to the current balloting process or the relevant legislative requirements for voting.”

However, because of the need to proceed with caution, in view of the high stakes, some respondents have proposed a more incremental approach. For example, the UKCRC suggested that: “As always, introducing new technology does introduce new attack vectors and these need to be understood and mitigated. E-balloting systems, if designed poorly, can fail in a much more devastating manner compared to classical systems.”[36] Professors Ryan and Schneider in the technology report[37] they prepared for me (see Annex 4) recorded as one of their conclusions: “It would make sense to start with smaller elections (for example, those involving a few hundred voters), rather than large ones (tens of thousands).”

The Electoral Commission also commented on the need for testing before going too far: “….for industrial action ballots, trust must be held by the trade unions and their members and employers. A key task in building trust will be to ensure that sufficient information is made available about any system being used and ensuring that any system has been independently tested and subjected to a certification or accreditation process. These measures will help to determine the degree to which the risks associated with e-voting have been addressed and thereby command necessary levels of trust.”

In designing any new e-balloting system it would be essential to refer to the relevant standards and ERS have helpfully observed that such a platform should be developed to industry standards, e.g. the server hardening standards the Centre for Internet Security publishes. ERS added that: “The system should also be regularly scanned for vulnerabilities by [an] 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 [Payment Card Industry Data Security Standard] PCI DSS standards for credit card processing).” They also noted the need for rigorous quality assurance procedures and processes and the need for

[36] Information concerning how succeptible an e-balloting system can be to serious attack see Wolchok et al. Attacking the Washington DC Internet Voting System, 2012. In Proc. 16th Conference on Financial Cryptography and Data Security,

[37] Mark Ryan and Steve Schneider. 26 July 2017: ‘Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action’

certification in quality management and security, such as ISO 9001[38] and ISO 27001[39].

Finally, it is worth recording that EEF urged that any e-balloting system should be capable of allowing the voter to register a vote but to effectively abstain in the same way they could with a postal vote. EEF argued that "…the functionality of electronic balloting would need to be the same as a postal ballot."

Comment

6.3 I understand the impatience of trade unions and e-balloting providers and proponents, but I am conscious of the many threats confronting internet users and the temptation the web presents to wrong doers.

6.4 Security is key where industrial action ballots are concerned. I acknowledge the need to avoid over-engineering the system and setting the bar too high. I also accept that in drawing up any code of practice for scrutineers and IT providers one should take a flexible approach and avoid being overly prescriptive, so as not to make both Code and technology obsolete. Nonetheless, with the need for security in mind, I am struck by the cautionary note sounded by the UK Computing Research Committee and the Electoral Commission. I am also mindful of the point about starting small made by Professors Ryan and Schneider in the technology report[40] I commissioned from them. I am conscious that trade unions already use e-balloting for non-statutory ballots but I believe we need to see the technology thoroughly proven under stringent test conditions for something as important as a trade union ballot on industrial action before it is deployed. For this reason I propose that it be tested using non-statutory ballots.

6.5 Non-statutory ballots are used by the trade unions to consult their members on issues. They are a method of testing the strength of feeling. The unions organise the ballots according to their rules, but all members affected by the issue concerned are given an opportunity to vote. However, if the union has constructed such a ballot to test opinion about taking industrial action they need another formal ballot under the trade union legislation to actually proceed.

Q9. How will e-balloting change the scope for industrial action and how does that affect the public interest?

Twenty seven respondents answered this question. A third believed that e-balloting would change the scope for industrial action, with 59 per cent of these respondents referring to increased voter turnout. The remaining two thirds of respondents either considered that e-balloting would not affect the scope for industrial action or were undecided.

[38] IS0 9001 is a quality management systems standard to help organisations meet the needs of their customers and stakeholders.

[39] ISO 27001 is an information security standard for measuring and evaluating an organisation's information security system management

[40] Mark Ryan and Steve Schneider. 26 July 2017: 'Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action'

Among the questions to be considered here are if e-balloting were to drive up participation what effect that might have on industrial action and, in particular, industrial action in “important public services” (see chapter 1, paragraph 1 regarding the Trade Union Bill (which became the Trade Union Act 2016)). The TUC and unions in general picked up on these points. Another issue is whether if an increased turnout were triggered that would mean a given strike would be perceived by the public as being more democratic and valid, and thus more acceptable and more worthy of support.

The TUC and the unions generally held the view that e-balloting could potentially increase turnout and help them meet the statutory thresholds. For example Unite said: “Unite has no doubt that e-balloting will increase turnout and participation in all union ballots.” Others were similarly minded. The Employment Lawyers Association (ELA) commented: “ELA believes the convenience and immediacy of e-balloting is likely to increase turnout.” However, as we saw in relation to question 3 (Chapter 5), not everyone who responded thought turnout would rise. An individual respondent observed that: “There is no evidence that e-balloting will ether increase or decrease turnout of any significance.”

Given their certainty that participation would increase with e-balloting, a number of respondents believed that this would change the public’s perception of particular industrial action. For example WebRoots Democracy observed that: “It is difficult to see how e-balloting could change the scope for industrial action, however through increased participation, it could increase the perceived democratic legitimacy of any decisions taken on industrial action which can only be positive for society.” The BMA made a similar observation.

Smartmatic commented that: “Any ballot or election suffers when turnout is low whereby wider relevant group [sic], and in the case of industrial action ballots, the general public, have to live with the decisions of a small minority. Unequal turnout matters because it reduces the incentives for Governments, organisation and trade unions to respond to the interests of non-voters and threatens the central claim of democracy.” However, not everyone agreed. For example, the Fire Brigades Union (FBU) commented in their response that it did not foresee any significant change in the scope for industrial action: “FBU members exercising their democratic right to pursue industrial action have consistently exceeded existing balloting thresholds……In our experience, the public have been highly supportive of the FBU efforts to defend our members’ interests and the service they provide to the public.”

In this context one might next ask whether strikes might become more likely if e-balloting were introduced. In my roundtable meetings a number of trade unions were keen to impress upon me that by no means all industrial action ballots led to industrial action. They were often simply a tactic towards a desired outcome. This was reflected in some of the responses from the unions. The consensus among the trade unions was that an industrial action ballot was always a last resort, but on some occasions it was the only way to resolve a dispute. There was agreement that sometimes the mere threat of industrial action led to a breakthrough.

The TUC observed: “Where negotiations are unsuccessful, unions may decide to run a ballot for industrial action. Ballots serve an important purpose by concentrating employers’ minds and demonstrating the strength of feeling amongst the workforce. The vast majority of industrial action ballots do not lead to industrial action.” They added that: “….in general the TUC does not believe balloting will increase the levels of industrial action in the UK. It certainly will not extend the circumstances where industrial action would be potentially lawful, as it is tightly regulated by separate rules on trade disputes.”

Many respondents felt that participation would increase but that industrial action would not rise as a result. Others thought that participation would not increase. While e-balloting might encourage people to vote, they would not necessarily vote in favour of industrial action; for every person who found that e-balloting encouraged them to vote and who subsequently voted for industrial action, there could well be another person who, likewise, was encouraged to vote but voted against it.

On the speed of the process, the UK Computing Research Committee (UKCRC) observed: “….a sequence of e-balloting instances can be run over short periods of time or even concurrently on different election options.” On the face of it, if just e-balloting were available, this would certainly interfere with the current dynamics of a dispute in that the time for negotiations would be shortened. This could mean that there was no longer enough time to reach agreement before action began, which would not be in the interest of any relevant party.

However, I am mindful of what the unions told me in my roundtable sessions and is repeated above, i.e. that the threat of industrial action is often a tactic and a means of seeking negotiation. Thus while the process might be quicker it is not necessarily the case that anyone (or by no means not everyone) would be readier to take action than under the postal approach. In any event, I am not advocating that postal balloting be discarded and nor could it be, as it is a legal requirement. Should electronic balloting be introduced the relevant legislation would require that postal balloting be retained so as to offer trade union members a choice of channel. If this were done balloting would still have to proceed at the pace of a postal ballot in order that all votes could be counted before a decision was made. Therefore any question about whether the negotiation process might be foreshortened would be academic.

It occurs to me that some people might need training to use e-balloting, for example people with disabilities and those with learning needs, and possibly some older workers too. This is something which the UKCRC made a passing reference to in their response: “E-balloting can be easier and faster to execute, assuming people are properly trained for the system and they have a reasonable level of familiarity with PC/smartphone/table devices.” Any training needs should be the unions’ responsibility.

There is also the issue of social media and its effect on balloting. Political blogs are rising in popularity and are eclipsing traditional media channels in terms of achieving wide readership. For example, the three most read stories about the 2017 general election between 17 April and 31 May were from such sources. The most read story was accessed 102, 655 times.[41] In the roundtables the trade unions told me how much they use social media to drive discussion about their agendas and, not least, industrial action decisions. Social media enables them to advise their members as to how to cast their decisions, which, for the avoidance of doubt, is not the same as coercion. It is also open to employers and others to use social media in order to counter the arguments in favour of industrial action. The use of social media communications goes hand in hand with the e-balloting processes. An election services provider noted that: "What will drive turnout increasingly will be the issue that is being voted on and/or to some extent the pre-election engagement that is undertaken ahead of an election with the voters, i.e. the marketing and promotion of the election."

The UKCRC said in its response: "…e-balloting can be directly combined with other tools such as online forums that assist union members deliberating and forming opinions about relevant union matters. Voting and deliberation can thus be considered to be part of the same platform hence streamlining the preparatory process. Given the above, one might speculate that this enhanced flexibility can allow for a more active involvement of union members in consultations and hence an increased level of interest in union matters."

Comment

6.6 Whether industrial action would become more common if e-balloting were introduced remains to be seen. Certainly the trade unions tend to argue that relatively few votes for action actually lead to action being taken, as a strike is in no party's interest. A test of e-balloting of the kind I have in mind, using non-statutory ballots, would not be determinative as one could only find out the answer if industrial action ballots in accordance with the 1992 Act were involved. (The same is true about whether participation would increase of course, but the use of non-statutory ballots could provide an indication). However, if e-balloting were ultimately permitted and there was an increase in positive decisions for action, it would be hard to judge whether this was attributable to the introduction of e-balloting or some other factor, such as the reason for the industrial action.

6.7 Social media would undoubtedly have a part to play if e-balloting were introduced. However, it is a factor in daily life already and is currently one of the tools that trade unions and others use in communicating about employment matters. If e-balloting were introduced it might cause a quickening in the pace of the use of social media but in any case it is now a fact of life, as illustrated by the rise of digital media.

6.8 It is reasonable to suppose that e-balloting might, to some extent, alter the way some individual trade union members - who currently use postal balloting - go about informing themselves before making a decision as to whether to vote for industrial action. Given the concern felt in some parts of the trade union movement (and expressed to me in

[41] DIY political websites: new force in shaping the general election debate: https://www.theguardian.com/politics/2017/jun/01/diy-political-websites-new-force-shaping-general-election-debate-canary

some of my roundtables) about the relative disengagement of some members, e-balloting might also be a means for the trade unions to reconnect with some of their membership. I recognise that this by itself, however, is not a reason for introducing e-balloting.

Q10. Are there any other risks or challenges associated with e-balloting, not identified above? How might they be mitigated?

Twenty eight respondents answered this question. Approximately 7 out of 10 identified risks or challenges associated with e-balloting. Issues focusing on security were the most widely cited concern. The majority of respondents making this point either underlined their previous arguments or elaborated on the theme of security.

A number of respondents (for example the TUC, the Royal College of Midwives and the Fire Brigades Union) emphasised that while security risks existed with e-balloting they were also present with postal balloting. The TUC summed up the sentiments of a number of unions in saying: “It is important that the risks associated with union ballots are accurately assessed and not overstated. In our opinion the risk of third party intervention or interface in union ballots are low, certainly as compared with public elections for MPs or local councilors.” Scytl remarked that: “The presence of a security risk does not mean that a voting channel is vulnerable; what makes a system insecure is the lack of security measures that properly mitigate the risks. In online voting, advanced security protocols and frameworks are of paramount importance in ensuring risk mitigation and secure elections.”

Popularis underlined the human factor as the biggest risk with e-balloting. Given the potential for hacking and malicious spam mail, Popularis considered e-voting to be more susceptible to human interference than postal voting.

Distributed Denial of Service also requires consideration. Smartmatic helpfully defined the term in a technical paper attached to their response: “Distributed Denial of Service (DDoS) attacks are cyber-attacks in which a perpetrator seeks to make a network resource or service unavailable to its intended user, such as to temporarily or indefinitely suspend or interrupt services. A DDoS attack is normally accomplished by overwhelming the target resource with superfluous traffic or network requests, which overload the target service and prevent it from fulfilling legitimate requests and processing valid requests.” Smartmatic believed such attacks could be sufficiently guarded against with the right technology and also pointed to the fact that e-voting offered a window of opportunity to vote, say seven to ten days before the poll closed, thus mitigating against a sustained attack on polling day.

An employer group raised the subject of whether the employer’s IT system would be used in any e-ballot which might be arranged. They had concerns about this and said: “….(a) there would be a large cost for establishing company email addresses to facilitate voting if the trade unions would not be willing to use these email addresses for other matters, which we anticipate is the case: (b) also we would be concerned that the unions would require those email addresses to be maintained and operated on terms that would be expensive and burdensome (c) the trade unions would accuse employers of intimidating their employees if they have access to electronic communication channels.” On the other hand, for their part, Usdaw commented that ensuring employers were excluded from the balloting process tended to give members confidence in the independence of the outcome and added: “Therefore, Usdaw is unlikely to deliberately call upon the use of employer’ IT systems to run a ballot.”

Finally, Scytl pointed to the need for a voter education programme, so that voters could use e- balloting properly. They said: “Apart from the technology-related challenges, the issue of voter education is cited as a concern. A lot of time and money must be invested to ensure that the public is aware that electronic voting is an option and that voters are able to understand and use the on-line system to cast a ballot. Without correct marketing and advertising it will be difficult to engage electors.”

Comment

6.9 Few people would deny that there are security issues with e-balloting. Where people tend to differ is on how seriously these risks need to be treated and the degree of protection needed against them. As we have seen, for some groups e-balloting is as straightforward as internet banking, but, for the reasons I have given earlier in this document, I profoundly disagree. Security is paramount. However, I understand that the bar should be set at a proportionate security height.

6.10 It follows from the above that I quite agree with those respondents who argue in relation to e-balloting that, whether because of potential intervention by a nation state, an organised group or just a single individual focused on disrupting a ballot, a Distributed Denial of Service and other forms of hacking and general interference are a serious risk and ones that need to be militated against effectively.

6.11 A voter education programme might well be useful and, in particular, might assist disabled people, less IT literate older trade union members and those with learning needs. However, I believe the cost of any such programme should be met by the trade unions themselves.

Q11. How might other non-technological processes need to change, such as the role of the scrutineer, if e-balloting were made available for industrial ballots?

Twenty seven respondents answered this question. The need for scrutineers to adapt effectively to the process of e-balloting was referred to most frequently. Two issues figured strongly - scrutineer standards and scrutineer competency skills and services.

Scrutineer standards

Unsurprisingly, no one called for an end to scrutiny. Rather, the responses tended to reflect what was said in the roundtables, that the scrutineer needed to be retained and their role adapted to e-balloting. Respondents were still very much looking to the independent scrutineer as guarantor of the integrity of the voting process. The UK Computing Research Committee envisaged the scrutineer becoming an integral part of the technological system. They said: "….a number of state of the art e-balloting systems support end-to-end verifiability and additionally have the capability to facilitate delegation to a third-party for scrutiny. In this way the role of the scrutineer can - in principle – be ported to the e-balloting setting."

The TUC was clear that an independent scrutineer was essential (as were a number of the unions in their responses). As with postal balloting, the scrutineer would need to report on each electronic ballot and the TUC recognised this.

Should e-balloting for industrial action eventually be introduced it will be essential that scrutineers and, where different, e-balloting system providers, are approved by the Government. The TUC drew attention to the existing list of approved scrutineers[42] for which BEIS is responsible. The inference appeared to be that they would expect to continue to choose from this list and that BEIS would need to re-visit it to ensure that those listed had the requisite skills and could meet the necessary standards required to scrutinise an e-ballot or provide a suitable IT system.

On a practical point, the CWC pointed out that: "Not all qualified people approved to act as independent scrutineers currently offer e-balloting. This may reduce the choice of scrutineers available as not all will have the means and technology to provide electronic balloting operations."

Rightly, the TUC and some of the unions envisaged a code of practice or guidance being issued on the scrutiny process and cautioned that this should not be overly prescriptive. They added: "Instead they should be sufficiently flexible to ensure that it is both practical and cost effective for unions to use electronic voting systems and that members who vote electronically are not disadvantaged as compared with those using postal votes."

Skills/services

Electoral Reform Services (ERS) took issue with the statement I quoted in the Call for Evidence from The Open Rights Group about how easy it might be to perform adequate scrutiny for online ballots. While agreeing as far as public election ballots were concerned, ERS did not think the statement applied to industrial action ballots. In that context ERS believed they had demonstrated through their expertise and experience over 15 years of online voting that it was possible to monitor "the pattern, timing and frequency of votes being cast, internet protocol (IP) addresses etc., so that suspicious activity can be identified and investigated for evidence of malpractice. One advantage of multi-channel voting projects, postal and online, is that the voting patterns of the different channels can also be monitored."

[42] Trade Union Ballots and Elections (Independent Scrutineer Qualifications) (Amendment) Order 2017; Recognition and Derecognition Ballots (Qualified Persons) (Amendment) Order 2017. (The list of approved scrutineers was updated in autumn 2017, and now includes Electoral Reform Services, Involvement and Participation Association, Popularis, UK Engage, Mi-Voice, and Kanto Elect).

ERS added that they were able to replicate through their online voting systems the approach they took with paper ballots, keeping separate the list of voters from the voting papers and inspecting the list only if an investigation was required. They said that: “The personal voter details used for the distribution of voting codes are kept separate and only connected to the voting data when required. This separation of data minimises the risk that the secrecy of an individual member’s vote will be compromised.”

The skills of a scrutineer who had hitherto only handled postal balloting who then proposed to cover e-balloting as well would need to expand considerably to embrace the technological challenge involved. Among others, the Electoral Commission recognised this and summed up what would be needed: “Clearly, any introduction of e-balloting will require the scrutineer to develop a sufficient level of knowledge of the relevant technology and software to deal with any issues in an informed and effective way in liaison with suppliers, and to keep trade unions and employers fully informed as to the progress and resolution of those issues.”

The standard the scrutineer is required to meet is clearly key to any e-balloting system. If e-balloting were introduced and the scrutineer could not detect any flaws that existed, balloting would be called into question, defeating the entire enterprise. The Employment Lawyers Association (ELA) recognised this in noting that: “The Government may need to consider the extent to which an independent scrutineer would make a report about whether the ballot has met the relevant legal requirements without an understanding of how the E-balloting system had operated and the technology used.”

The service levels expected of the scrutineer/service provider for an e-balloting operation would be different from those required for a postal system. Popularis pointed out that an extensive operation might be required. They said: “It is possible that the role of the scrutineer will require a change to 24/7 support and helplines to support and help members having difficulty accessing the system. The demand now is for instant responses, and that creates a pressure to provide them. Currently all queries and complaints are checked, such as for non-receipt of a ballot paper by post, and great care is taken in doing so. The scrutineer would need to be assured that the email addresses supplied were accurate and up to date, and that any requirements for whitelisting through secure sites have been undertaken prior to the ballot.”

Finally, as touched on earlier under question 10, the voter dimension should also be taken into account when considering adaptations that might be required to pave the way for e-balloting. Scytl observed that an important change that might be required could be: “The need for adequate technical skills as regards voters to use online voting, e.g. familiarity with technology, ability to use a web browser and an internet-connected device, ability to use emails etc.” However e-voting would not be mandatory.

Comment

6.12 Clearly the scrutineer’s role (and their eventual report) will be key if e-balloting is ever deployed. One would want the scrutineer to be able to perform the same checks and controls as they do with a postal ballot but the task becomes much more complex in the technological sphere. It may be that the current scrutineers have the technical skills to be able to detect any security risks and incidents of interference as well as those needed to monitor proceedings. However, for the purposes of the trial, and possibly later, I do not believe that we can simply take on trust that the scrutineer will be omniscient, even though we currently hand the process over to them under the postal system. There are too many technological variables which can go wrong with an e-ballot.

6.13 Accordingly, longer term - if e-balloting were introduced - I believe the Secretary of State would need to update the existing code of practice for scrutineers and set the standard, i.e. the skills, services and capabilities, which would be required of an e-ballot scrutineer and associated technology providers. The trial of e-balloting I recommend would help to flag up what would be needed.

6.14 Consideration will also need to be given to whether there should be further third party assurance, over and above that of the scrutineer, regarding the electronic balloting systems used both during any trial and in any subsequent roll out of e-voting. A trial would be a good opportunity to test how such assurance might work and what might be feasible.

6.15 I am aware that third party assurance is required in Estonia and Denmark. For example, in Denmark, many trade union ballots, including those for industrial action, are conducted by a balloting service provider called Assembly Voting, with Deloitte acting as auditor. Deloitte have the necessary cyber expertise to determine whether relevant IT systems have been hacked or the ballot otherwise interfered with. However, there is a cost for such audits which varies according to the number of trade union members who are involved in the ballot. Thought would be needed as to what level of audit was required, which along with the number of voters involved would help to determine the price. A number of scenarios can be envisaged as to how third party assurance might work. For example:

(a) Each ballot might be conducted by the scrutineer alone;

(b) Only ballots involving “important public services”, as defined by the Important Public Services regulations 2017[43], might be overseen by a suitably qualified and approved third party assurer and/or perhaps only ballots involving trade unions with a total membership above a certain threshold; or

(c) All ballots might receive third party assurance.

[43] Important Public Services Regulations, 2017: http://www.legislation.gov.uk/ukdsi/2017/9780111151976/contents.

6.16 An expert panel would be needed to oversee any trial and, in particular, review handling of the scrutiny process in order to learn any lessons and build these into the programme. My view is that the panel should comprise a cyber expert (perhaps an academic could best fill the role), a legal expert, an accountant, an employer representative and a trade union representative.

6.17 The need for any learning programme has been addressed under question 10.

Q12. What costs are associated with the technological options around e-balloting and also non-technological mitigations?

Twenty four respondents answered this question. Two thirds considered that e-balloting would increase certain costs while reducing other expenditure. Costs are not something that figured highly during my roundtables, however, a number of respondents have answered this question. The evidence submitted covers a range of topics. Certainly one aspect worth considering is what the right amount of resource might be for facilitation of a test of e-balloting technology. The cost could be quite substantial. In recalling the 2007 e-voting pilots the Electoral Commission touched on the need to make proper provision: "The 2007 e-voting pilots were expensive, principally because they were conducted as one-off projects involving the set-up of complex IT systems which were implemented in very short timescales. In addition, the level of e-voting usage did not allow economies of scale to be achieved."

A considerable amount of thought would be needed for preparation for any e-balloting test, something EEF recognised in saying: "Electronic balloting would also need to allow for recounting as well as some form of verification of the votes cast. There are therefore some significant areas to address in principle before the areas could be progressed to a consultation."

More generally, and perhaps more obviously, there are the ongoing costs for trade unions which would need to be considered if e-balloting were ever to be fully deployed. A number of respondents pointed out that there could be large upfront/ sunk costs for providers which would probably be passed on to the trade unions to absorb too. Popularis commented: "In a larger ballot, the costs for e-balloting will be less than postal balloting due to the rising costs of postal. But it does need to be a large ballot. In industrial action ballots, often involving certainly less than a thousand members, and often only a very few hundred, it is difficult to provide an e-ballot as a cost effective alternative to a postal ballot."

However, there would probably be economies for the unions to take advantage of. Smartmatic said: "Since its inception, the internet has proved to be a cost-effective platform upon which to deliver all manner of services. The internet offers huge economies of scale which have hitherto been experienced in other 'network' based services (e.g. mail) and this economy extends into the use of the internet for voting."

A number of other respondents picked up on the savings the unions would make from not always having to use the postal system. For example, when I met Electoral Reform Services they pointed out the difference in cost between sending a few thousand text messages compared to sending letters and noted the ease at which texts could be sent. The Fire Brigades Union commented: “It is likely that unions will incur additional costs should the use of electronic voting become an option for statutory ballots, owing to investment in new ICT systems and the costs of contracting balloting agencies to run ballots. Nevertheless, we anticipate that use of electronic voting will reduce postal costs for unions in the medium-long term.” A number of other trade unions commented along similar lines.

Scytl observed that: “Whilst for the most part the aim is to reduce cost within the election process some unique costs will be generated, such as the cost of raising awareness of the platform to the electorate. A further consideration will have to be made for the cost of establishing the design of the voting interface. Whilst the design of the voting client is simple, it will require a design house to set out the experience and will have to be built to work across all devices. Furthermore, it is likely that the overall party responsible for hosting the delivery of the platform (i.e. the trade union) will have to provide both a web based Q&A or a call centre support – again it is probable that the cost of these services can be met within existing budgets as the platform acts to remove costs in the existing system.”

Where an e-voting system was provided from scratch there would be relatively high costs. While pointing out that it was not possible to provide indicative costs as there would be so many variables involved, Smartmatic helpfully detailed the typical areas of spend required (please see the following table).

Smartmatic's assessment of the typical cost elements associated with e- balloting

Phase	Activity	Detail
Design/Procurement	Request for information – Call for evidence	Understanding of the market and review of success cases for online voting
	Definition of business and technical requirements	Ratification of business case, creation of technical solution requirements
	Procurement of solution	Request for Tender/proposal
Acquisition	Licensing	Licencing off the shelf e-balloting solutions or components from vendors
	Engineering and development	Customisation of solution to meet business and/or technical requirements
	Quality Assurance and testing	Ongoing quality assurance and testing to ensure business and technical requirements are being met
	Staging solution	Implementation of staging platform for internal test and customer sign off
	User acceptance testing and sign-off	Sign-off of the solution by the customer
	Acquisition of operational infrastructure	Acquiring operational datacentre and networking for running the platform
	Implementation and project management	Services associated with setting up the production platform
	Logic and accuracy testing	Ensuring the solution meets the election business rules
	Security and penetration testing	Ensuring that the system is appropriately protected from possible external and internal threats
	Independent system certification	Certification and approval of system with independent third party
	Final customer sign-off	Final sign-off and handover to customer
Operational (per election) costs	Election definition	Definition of ballot and creation of voter list
	Credential distribution	Distribution of voting credentials (mail, email, SMS)
	Tabulation and counting	Resource to oversee tallying of results
	System support	Resource allocated to support the solution

Without being overly prescriptive, in order to avoid stifling innovation and leaving any system underpowered and outmoded, the Secretary of State would need to specify some general standards that providers and scrutineers would have to be capable of meeting. To some extent, therefore, the Government will have a hand in establishing the costs involved. The CWU noted that: “There are expenses associated with creating the technological infrastructure for e-balloting. These may be prohibitive for smaller trade unions or small-scale industrial disputes. This is why it is important that legislation allowing e-balloting should not be overly restrictive or bureaucratic.”

In addition to the overall platform there would be the cost of the means of accessing it for the voter. However, as the UK Computing Research Committee noted, the means of access are already in the hands of much of the population in the form of mobile phones, computers and tablets. “Furthermore, it is also possible to retain some of the potential benefits of e-balloting by using a hybrid approach between e-voting and postal voting where, say, paper ballots are distributed by post containing personalised vote codes that can be submitted via very lightweight devices (even the regular telephone). In this case, the client-side costs become minimal.” Naturally, of course, postal voting will remain an option.

Finally, there is the question of whether the employer would face any costs. I believe any employer costs should be minimised. Any such costs seem most likely to arise where the employer chose to allow an e-ballot to take place using their IT system and agreed to the lifting of firewalls and any other minimal expenditure to facilitate matters.

Comment

6.18 If a trial is considered appropriate, it will be necessary for BEIS to make adequate provision for e-balloting trials to take place including the appointment of the expert panel (referred to in paragraph 16 above) to oversee the trials and evaluate the outcome.

6.19 Trade unions already use e-voting (for non-industrial ballot issues) and other organisations also use internet voting platforms. It is likely that if allowed to use e-balloting for industrial action ballots, unions would use bespoke e-voting services, either via an approved independent scrutineer or via an independent scrutineer hiring an e-voting provider. However, such systems would first have to meet the security standards set by the Secretary of State which should include compliance with a new code of practice.

6.20 It has not been possible to access any information about the precise costs of e-balloting services or industrial action ballots (it is likely to depend on the size of the ballot). However, it is assumed that the cost would need to be at least broadly equivalent to the cost of postal ballots for unions to consider them a viable option. The costs of an internet plus postal ballot would likely be higher, though unions would still have the option of having a postal only ballot.

Chapter 7

Overall Conclusions

7.1 My meetings and discussions revealed a large measure of support for the concept of e-balloting alongside the existing statutory requirement for trade union postal balloting for industrial action. I was also struck by some who felt that e-balloting was without any risk, or that it was akin to other existing balloting matters or use of a bank card at a cash point machine.

7.2 Whilst I fully recognise the potential benefits and opportunities e-balloting might bring I have concluded that it would be equally wrong to dismiss and over simplify the risks. There are some good examples of telephone/electronic balloting in common use ranging from popular television programmes to more significant political leadership and Board decisions, each of which has relevance to the voter and the outcome. However, this review has reconfirmed my view that there is a broad spectrum of importance where ballots are concerned, which, I would argue, spans from media entertainment through to municipal decisions of local elections, general elections (and referenda). At the latter end, the secrecy of the vote and protection against coercion are paramount.

7.3 I do not consider that balloting for industrial action is equivalent to general elections, but I believe it is not far behind given that industrial action can have significant implications for the individual voter, the trade union, the employer and often the public. It is important to ensure that all stakeholders would be able to have confidence that a decision reached via an e-ballot had been arrived at without any malpractice. Because such confidence is key there is a proportionate risk of potential disruption to the outcome of the ballot result from nation states and others who might be motivated to interfere.

7.4 Some I spoke to felt that the ‘security’ bar should not be set higher than that achieved by the current postal balloting process. I recognise this, but in so doing I am also aware of the need not to reduce the level of secrecy surrounding the personal vote. Nor should we lose sight of the enhanced risk of cyber-attack when considering e-balloting processes.

7.5 Whilst I heard some frustration at any delay in implementation in e-balloting for industrial action I am also conscious that putting in place a less robust e-balloting process provides a significant risk of challenge and failure. Such failure would be likely to result in e-balloting being brought into disrepute and the potential suspension of such systems for many years.

7.6 For the above reasons I did not find a compelling case to move directly to the introduction of e-balloting for industrial action ballots. However, if the Government were minded to consider deploying e-balloting for industrial disputes it would be sensible to carry out some tests first - over a reasonable period - in order to determine whether it can deliver a result its stakeholders can have confidence in. Such tests could also indicate whether e-balloting would increase voter participation.

7.7 Before deciding on whether there should be e-balloting for industrial disputes, there should be testing of e-balloting for non-statutory ballots. Any such test should be limited to exploring the potential for extending e-balloting to voting for industrial action and for no other purpose. Thus any test or subsequent trial would not be a precedent for wider application in general or municipal elections.

7.8 I am aware that trade unions already use e-balloting for non-statutory ballots but they do not do so under the stringent test conditions I believe are necessary and nor has the department for Business Energy and Industrial Strategy monitored or evaluated such balloting.

7.9 It is unclear which method of e-balloting would be most effective, therefore if e-balloting were trialled it would be sensible to test a number of different approaches and in a number of regions.

7.10 Under the Employment Rights Act 2004, in moving to other methods of determining ballots and elections held under the Trade Union and Labour Relations (Consolidation) Act 1992, postal balloting must be retained as an option. Accordingly, electronic balloting could not be made mandatory. However, regardless of the statutory requirement, there are sound, practical reasons to retain postal balloting, for example, because of the potential for an electronic balloting service to be denied by hacking or malware or to become unavailable owing to a malfunction or technical fault. There is also the need to make provision for those with protected characteristics who may have difficulty in accessing information technology. Therefore if e-balloting were trialled it would be reasonable if it were done alongside postal voting.

7.11 Trade unions should be free to choose which independent scrutineer to contract with to conduct their e-ballot. Such scrutineers should first be accredited by the Secretary of State for the Department for Business Energy and Industrial Strategy. This is currently achieved by the unions being required to choose prospective scrutineers from a list of approved independent scrutineers entitled to carry out trade union ballots and elections and qualified independent persons for the purposes of trade union recognition. If e-balloting were to be introduced, consideration would need to be given to the criteria scrutineers should fulfill, and in particular those scrutineers who intended to offer e-balloting services. For example, given the need for secrecy and robust systems an independent scrutineer would have to be able to offer ‘end-to-end verification’ by being able to monitor that there had been no interference with the vote and that in each case the integrity of the ‘ballot box’ has been respected and a valid ballot has been conducted.

7.12 I consider it appropriate that if e-balloting were to be introduced, the Secretary of State should satisfy himself/herself that the scrutineer is able to fulfil the requirements for e- balloting. To this end it would be appropriate to decide what the code of practice for industrial action ballots should contain in order to take account of e-balloting. The code could also introduce any level of assurance/audit that might be deemed necessary, in particular in the event that a third party audit of the scrutineer is required. This is particularly important in relation to the cyber-attack aspects of e-balloting.

7.13 An e-balloting code of practice should be drawn up in light of the e-balloting trials by an expert advisory panel, appointed by the Secretary of State. Such a code of practice would need to be in place before long term use of e-balloting was ever approved and would ultimately be required for ballot coordinators, scrutineers, and third party assurers and trade unions to follow. The code of practice should be similar to that governing paper based ballots.

7.14 During any agreed trials of e-balloting it would be important to consider the seriousness of the threat from hacking/cyber-attack and decide if such an attack can be sufficiently mitigated against to an acceptable level. It might be considered that industrial action in relation to important public services as defined by the Important Public Services Regulations 2017[44] might be at most risk from external interference. During any trial of e-balloting for non-statutory ballots it would be possible for the Secretary of State to commission 'ethical hackers' to test the robustness of the systems used.

7.15 It would be helpful if any trials that took place used a variety of different ways and methods of voting, including via the remote use of stand-alone, individually held smart phones, computers and tablets. I leave it to the Secretary of State to consider whether the use of employers' IT systems (where this might be agreed) should also be examined in any test. In every instance, trade union members would first have to be asked to indicate whether they wished to vote by electronic or postal means. It would be especially important to assess the impact on disabled people and other protected groups during the trials.

7.16 The Secretary of State would need to decide how many ballots would need to be tested in order for a fair trial to be conducted. He or she would also need to consider where the trials should take place, in which sectors and over what timescale. It would be for the trade unions to decide whether to participate.

7.17 The protection of the integrity of the secret ballot from intimidation and coercion is essential. In this context I was encouraged to note the practice in Estonia and Denmark where to counter potential coercion voters are allowed to vote (or 'revote') any number of times before the deadline by which the ballot closes, however only the last vote cast counts. It was reported that such a solution also permits a period of reflection in the period of the ballot remaining open, rather than a single early decision being made. In the case of Estonia, an e-vote is subordinate to a paper ballot so that once someone has cast a postal vote (or polling station vote) no further voting is possible. If a trial is agreed I support the inclusion of these principles in e-balloting for industrial disputes.

7.18 I received mixed views for and against voters being able to verify that a vote has been received as cast. It can be argued that (in a similar way to allowing voting any number of times outlined above) it is an added feature of e-balloting not previously available. I therefore recommend that any trials also test this facility for subsequent evaluation.

7.19 Sufficient time would need to be allowed in order to plan any proposed e-balloting tests to meet the above criteria. At least six months planning time would be required from the point that the Secretary of State decided to give the go ahead and the tests'

[44] Important Public Services Regulations, 2017: http://www.legislation.gov.uk/ukdsi/2017/9780111151976/contents.

commencement. During this time a standard for scrutineers and others to follow (as a precursor to a code of practice) could be developed.

7.20 Finally, as outlined above, any test to determine whether e-balloting could fulfil the rigorous requirements demanded in the context of an industrial action ballot would need to be thoroughly evaluated.

INDEPENDENT REVIEW OF ELECTRIONIC BALLOTING FOR INDUSTRIAL ACTION: RECOMMENDATIONS

Recommendation 1: E-balloting for industrial action ballots would only be capable of retaining public confidence if it were seen to be as secure and reliable as the current postal approach. In particular, e-balloting would need to be able to meet the required standard set out in Section 54 of the Employment Rights Act 2004; i.e. it would need to ensure that those entitled to vote had an opportunity to do so; all votes cast would have to be secret; and the risk of any unfairness or malpractice would have to be minimised.

Recommendation 2: Owing to the number of unanswered questions surrounding e-balloting I am not persuaded that e-balloting for industrial action ballots can be introduced immediately. Instead I recommend that a test of e-balloting on non-statutory ballots is necessary as a preliminary step and that this would potentially be the basis for the Secretary of State to decide the matter.

Recommendation 3: Specifically, e- balloting should be trialed to see if it can meet the standard set out in Section 54 Employment Rights Act 2004. E-balloting should be introduced for selected non-statutory ballots across England, Scotland and Wales with the aim of evaluating, at least, the following:

- The resilience of e-balloting systems to cyber-attack and hacking. In this respect it is appropriate to use “ethical hackers” to test the robustness of systems used to support voting during any e-balloting trial;

- The operation and effectiveness of voter verification (the ability of voters to check that their vote has been received and cast according to their wishes);

- The alternative hardware options for casting a vote, including smartphones, emails, computers and, if appropriate, employers’ IT systems;

- Whether having ‘re-voting’ (multiple voting, last vote counts) provides increased protection from ballot malpractice and permits a period of reflection up to the close of ballot;

- Whether there is increased participation in a ballot as a result of e-balloting;

- How e-balloting might impact on people with disabilities as compared to postal ballots;

- The benefit of independent audit/assurance;

- Amendments that may be required to the BEIS approved scrutineer list to accommodate e-balloting;

- What additions might be needed to the code of practice for industrial action ballots to take account of e-balloting.

Recommendation 4: The providers of any systems used to trial e-balloting must be able to demonstrate that they are able to withstand cyber-attack/hacking from those who wish to cause disruption.

Recommendation 5: During any trial of e-balloting for non-statutory balloting, consideration should be given to the use of independent auditors to provide independent assurance for the end-to-end balloting process, including the risk of cyber-attack. It may not be considered practical to utilise external auditors for all industrial action ballots in addition to existing scrutineers. However, it might be thought reasonable to require such assurance for at least industrial disputes affecting 'important public services' as defined in the set of regulations known as the Important Public Services Regulations 2017[45]. Any expectation as to the role of an approved independent auditor could be included in the recommended code of practice.

Recommendation 6: In the event that a trial using e-balloting of non-statutory ballots is agreed, I recommend that the Secretary of State appoints an expert advisory panel whose terms of reference should include:

- Matters for evaluation that are to be part of the trial in addition to those identified in recommendation 3 above;

- The content and process for agreeing a subsequent e-balloting code of practice;

- Reporting back to the Secretary of State.

Recommendation 7: Should e-voting be adopted on a permanent basis, it will be important to retain the option of postal voting to allow the voter choice of channel, not least to ensure that an individual who is more comfortable with postal balloting is not denied that channel.

Recommendation 8: An independent evaluation would need to be carried out if any tests were conducted. It would seem appropriate if the cost of such an evaluation, together with any other test programme delivery costs involved, were met by the Government.

Recommendation 9: If e-balloting for industrial action were approved on a permanent basis the existing code of practice for industrial action ballots should be amended to set the standard that e-ballot coordinators, scrutineers, IT providers, auditors, trade unions and employers should follow in relation to e-ballots. The code of practice should cover the risks of cyber-attack and hacking.

[45] Important Public Services Regulations, 2017: http://www.legislation.gov.uk/ukdsi/2017/9780111151976/contents.

Annex 1

Terms of Reference for Independent Review of Electronic Balloting for Trade Union Industrial Action Ballots

Introduction

This review of electronic balloting for industrial action ballots conducted under the Trade Union and Labour Relations (Consolidation) Act 1992 follows the introduction of the Trade Union Act 2016. During the parliamentary debate on the Act the Government undertook to commission an independent review of the case for electronic balloting

Purpose

The review should take into account issues, including but not exclusively:

- The electronic and physical security of e-balloting methods, including risks of interception, impersonation, hacking, fraud or misleading or irregular practices;

- If any system can safeguard against risk of intimidation of union members and protect anonymity of ballot responses;

- The security and resilience of existing practices of balloting union members;

- The aims of the Trade Union Act 2016 to ensure strikes and related disruption to the public only happen as a result of a clear, positive decision by those entitled to vote;

Section 4 of the Trade Union Act 2016 specifies:

4. Provision for electronic balloting: Review and piloting scheme

(1) The Secretary of State shall commission an independent review, the report of which shall be laid before each House of Parliament, on the delivery of secure methods of electronic balloting for the purpose of ballots held under section 226 of the 1992 Act.

(2) The use of pilot schemes shall be permitted to inform the design and implementation of electronic balloting before it is rolled out across union strike ballots.

(3) The Secretary of State must consider the report and publish and lay before each House of Parliament his or her response to it.

(4) For the purpose of preparing the response under subsection (3), the Secretary of State must consult relevant organisations including professionals from expert associations to seek their advice and recommendations.

(5) The review under subsection (1) shall be commissioned within six months of the passing of this Act.

Glossary of terms and abbreviations

British Airline Pilots' Association (BALPA).

Biometric information – The unique physiological characteristics of a person that can be used for identification purposes and access control.

Blockchain technologies – A blockchain is a data structure that is used to maintain a continuously growing list of records or events, periodically grouped together into blocks. By design, blockchains are inherently resistant to modification of the data. Blocks are tied together using cryptographic operations called hashes. Once inserted, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks[46].

BMA – British Medical Association.

CWU – Communication Workers Union.

E-balloting – Electronic balloting: A system of voting in which the voter uses an electronic device to cast his or her vote.

EEF – The representative body for manufacturing.

EKRE party – The Conservation People's Party of Estonia.

ELA – Employment Lawyers Association.

ERS – Electoral Reform Services.

Ethical hacker – An individual or company who attempts to hack into a system on behalf of the owner in order to highlight potential weaknesses that could be exploited by malicious hackers.

GMB – Formerly known as General Municipal and Boilermakers Union.

Important public services – Public services that either: protect against loss of life or serious injury; maintain public safety or national security; enable economic activity across a significant area of the economy or; enable significant numbers of people to get to their

[46] Mark Ryan and Steve Schneider. 26 July 2017: 'Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action'

place of work. These public services, as set out by the British Government[47], include fire, health, education, transport and border security services.

Independent auditor – An accountant who helps to ensure the integrity of the auditing process by examining the financial records of a company with which he or she has no affiliations.

Mix-net – A procedure (known technically as a *cryptographic mixnet*) to shuffle and anonymise encrypted votes in a verifiable way (so the encrypted votes at the end match the encrypted votes at the beginning) analogous to shaking a ballot box of paper ballots.[48]

NASUWT – A teachers' union.

Nautilus – Maritime Union (formerly NUMAST).

Non-statutory ballot – A ballot that is not required by law and is used by trade unions for consultation purposes.

Postal voting – A system of voting in which ballot papers are distributed and returned via the postal system.

RCM – Royal College of Midwives.

Scrutineer – In the context of industrial action ballots the scrutineer plays an official role in the election or balloting process. The scrutineer manages the election or ballot, and is trusted to follow the appropriate processes, to maintain the privacy of the vote and to ensure the integrity of the election.[49]

Statutory ballot – An election or vote that is required by law. For example, trade unions are required by law to hold elections in order to fill certain positions within the union, such as President. They are also legally bound to hold ballots before taking industrial action.

Third party assurance – Independent professional monitoring by a Chartered or Certified Accountant to ensure that a particular operation is properly carried out or that a body has operated correctly.

TUC – Trade Union Congress.

TULRCA – Trade Union and Labour Relations (Consolidation) Act 1992.

[47] Important Public Services Regulations: guidance on the regulations https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/583582/Annex_A_Draft_40__guidance.pdf

[48] Mark Ryan and Steve Schneider. 26 July 2017: 'Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action',

[49] Mark Ryan and Steve Schneider. 26 July 2017: 'Using electronic balloting for industrial action ballots. A report for the Independent Review of Electronic Balloting for Industrial Action',

UKCRC – UK Computing Research Committee, comprised of leading computing researchers from academia and industry.

Annex 3

Engagement Events

List of meetings held by Sir Ken Knight

Sir Ken Knight met the following organisations and individuals in relation to the review:

CBI
Cybernetica
Danish Embassy (Assembly Voting, Dansk Metalworkers Union, 3F (United Federation of Danish Workers), Deloitte)
Deloitte
EEF
Electoral Commission
Electoral Reform Services
Employment Lawyers Association
Estonian National Electoral Committee
Mr Nicholas Finney
Local Government Association
National Centre for Cyber Security
Smartmatic
TUC (Frances O'Grady, General Secretary)
Webroots Democracy

In addition Sir Ken held 'round table' meetings as follows:

London: BEIS hosted 'Chattham House' meeting for all interested parties attended by: British Airline Pilots' Association, CBI, EEF, The Electoral Commission, Electoral Reform Services, IoD, IPA, Mi-Voice, Local Government Association, Professor Mark Ryan, Popularis Ltd, Scytl, UK-Engage, Unison, Unite

London: Eversheds/CBI hosted 'Chattam House' meeting for employers attended by: Arriva UK, Associated British Ports, DHL, Freightliner Group Ltd, Jaguar Land Rover

London: TUC hosted 'Chattham House' meeting for trade unions. Attendees included: British Airline Pilots' Association, British Medical Association, Electoral Reform Services, Royal College of Midwives, NUJ, Professor Steve Schneider

Glasgow: BEIS hosted 'Chattam House' meeting attended by: Babcock International, Electoral Reform Society, GMB, Law Society, Professor Steve Schneider, Scottish Government officials, STUC, Thompsons Solicitors, Unison

In Sir Ken Knight's unavoidable absence the review team also engaged as follows:

Cardiff: BEIS hosted 'Chattham House' meeting attended by Coleg Y Cymoedd, Electoral Reform Services, Eversheds Sutherland, TUC, Wales TUC,

Mr Graham Kirwan

Annex 4

Technology Report

Using electronic balloting for industrial action ballots

A report for the Independent Review of Electronic Balloting for Industrial Action

Mark Ryan and Steve Schneider

26 July 2017
Incorporating revisions made on 10 August 2017

1 Introduction

The Government has commissioned an independent review of the safety and security of conducting balloting for industrial action via electronic processes. In turn, the independent review has commissioned this independent report. In this document, we provide an independent, authoritative assessment of e-balloting technologies to contribute to that review.
The assessment takes into account the need to meet legal requirements for inclusivity, secrecy and minimising unfairness and malpractice.

2 Objectives

- To review the current state of the art in technologies to support secure, fair and usable electronic balloting, applied to the specific case of industrial action ballots.
- To document and evaluate the pros and cons, particularly in relation to cyber security and the reliability of the election outcome.

3 Review and analysis of the requirements

3.1 Industrial ballots

An industrial ballot is a ballot of trade union members, for example about whether to take strike action. The size of the election (i.e. the number of eligible voters) varies from a few tens of voters, to tens or hundreds of thousands. Industrial ballots today are conducted by a third party scrutineer, which sends ballots to union members through the post, and receives completed ballots and counts the votes. The ballot is typically open for a week or two. The scrutineer relies on receiving a list of eligible voters from the union. The employer is told how many eligible voters are on the list (and can complain if that number seems wrong), but because membership of a union is private information the employer is not given the list. The scrutineer is able to perform some crude analysis of voting patterns and times to try to identify anomalies.

From this description, one can immediately see that there are security vulnerabilities:

- It is hard to establish whether the list of declared eligible voters is correct.
- There are opportunities for interfering with ballots in the post, both as they are sent out and as they are sent back.
- Voters can pass blank ballots to others, either voluntarily or through undue pressure.

- Voters may be compelled to vote in a particular way.
- There may be opportunities to corrupt the scrutineer.

An important consideration when one considers electronic balloting is the desired security threshold. Given that the current system is postal balloting, we will take this is the baseline for comparison with electronic voting. This is rather a low baseline compared to what is normally sought in the academic literature on electronic voting, in which strong properties like incoercibility and universal verifiability (see section 3.3) are typically considered.

3.2 Threats to industrial balloting

A variety of different kinds of people may be interested in using hacking or coercion to try to change the outcome of the election, or to compromise the secrecy of voters, or merely to cause disruption to prevent the election taking place. Such people can include the directly interested parties (employers and employees), or politicians, journalists, or other kinds of commentators and observers. They can also include organised criminals and possibly also state-sponsored agents, that may be interested in industrial sabotage or damaging the economic well-being of the country. If an election is carried out electronically, attackers (especially in the latter category) may be sufficiently motivated and resourced to carry out attacks by producing specialised malware designed to interfere with voting platforms (such as laptops and mobile phones) and back-end voting servers.

3.3 Electronic voting for industrial balloting

Electronic voting has existed as a subject for academic research in computer science for about 30 years. The main properties sought are verifiability, and vote secrecy and incoercibility (defined below). These are properties that are needed for elections of national and international importance, like political elections. Unfortunately, these properties in their fullest form have not been achieved in the research literature. Industrial ballots may be considered smaller and lower-stake elections than political elections, although large industrial ballots could have substantial impact on the economic well-being of the UK. Their nature is different, and current practice is different, to political elections. Therefore, it is appropriate to look at a wider set of properties. We detail the requirements appropriate for the context of industrial balloting, starting with the strongest ones of verifiability, incoercibility and vote secrecy, and widening to other ones.

Verifiability. The outcome of the election should be independently verifiable by any independent observer. This can be split into three aspects:

- Individual verifiability (IV): a voter can check that her individual vote is included in the declared result.

Eligibility verifiability (EV): a voter or independent observer can check that only eligible voters votes have been included in the declared result.

- Universal verifiability (UV): a voter or independent observer can check that the computation of the declared result is correct.

Systems vary as to who is allowed to be an independent observer: it might either be any arbitrary individual or organisation with the verification information made public, or it might be independent auditors who carry out the verification but where some information is not made public.

The way this works in practice is that the voter or observer has software (for example an app on their phone) which carries out these checks, using encrypted data made available by the voting system server. The validity of the verifications does not rely on the server software, but it does rely on the voter’s software (that is, both the app that casts the vote, and the app that verifies the result).

Inclusion of verifiability in an electronic voting system recognises that any online system can become the victim of a cyber attack by a sufficiently resourced adversary. Verifiability provides a way to detect when the result of the ballot may have been altered by such an attack. Hence it provides a mechanism to ensure that that the result cannot be changed undetectably: a valid verification check for an election provides an assurance that the result is correct.

Vote secrecy and voter incoercibility. Vote secrecy means that the way any particular voter voted should remain private only to herself. Voter incoercibility means that a third party which attempts to force or persuade a voter to vote in a particular way should be prevented from effectively doing so. For example, this may be achieved by designing a system which:

● Is **Receipt-free.** This means that the system does not offer the voter any receipt which can later be used by the voter to demonstrate how she voted to a coercer. (Note that the term “receipt-free” is a bit misleading. The system might offer a receipt, but the receipt shouldn’t contain information which could be used by a coercer to deduce how the voter voted.)

● Allows **re-voting.** This means that a voter can vote multiple times, and only the last one will be counted. A voter who is coerced to vote a certain way can possibly later vote again, annulling her coerced vote. Note that this is only a partial mitigation against coercion, since a voter coerced in the minutes before an election closes might not be able to re-vote.

In the context of industrial action ballots the scrutineer plays an official role in the election process. The scrutineer manages the election, and is trusted to follow the appropriate processes, to maintain the privacy of the vote and to ensure the integrity of the election. The involvement of the scrutineer means that some of the voting system requirements listed above can be adapted to reflect the involvement of the scrutineer. In particular, the scrutineer is trusted to carry out eligibility verification checks and universal verification checks on behalf of voters and observers.

Resistance to attack. A voting system is necessarily a large system with many parts, and therefore exposes a large attack surface. The idea behind verifiability (mentioned above) is to ensure that certain kinds of attack (for example, attacks on the server that would cause the wrong result to be declared) are detectable. But not every system will have such strong verifiability properties; and client software can be attacked too; and there are other kinds of attack besides those that change the ballot. So it is very important that the system employ the highest available standards of cyber security in order to reduce its propensity to be attacked.

One particular kind of attack is called a **distributed denial-of-service attack.** This is one in which lots computers and devices around the world are taken over by a command-and-control centre, and made simultaneously to bombard an attacked server with requests. The intended effect is to overwhelm the server, preventing it from responding to legitimate requests. This kind of attack is very common, and very hard to defend against. The best defences are those put in place by the network operators (the ISPs) that mediate access to the victim server. In the case of voting, a useful defence is to extend the period during which the vote can take place (that gives more time for the ISP to deploy defences) and to allow voting-place votes.

Another kind of attack is **malware attacks on the voting platform** (i.e., the voter’s laptop, desktop, tablet or phone). Specialised malware could be written, aiming to target the voting app and to change the vote. In the context of industrial action, one consideration for unions is whether to use equipment provided by the employer or not; such equipment could potentially contain such malware. One can try to make this kind of attack easier to detect by requiring the voter to use two different platforms (say a laptop and a mobile phone) during the voting procedure. This would mean that the attacker had to attack both of them in a coordinated way, in order to remain undetected. This raises the bar for the attacker, but it doesn’t eliminate the threat completely. Malware aiming to compromise the voter’s ballot secrecy can also in principle be addressed in this way. See, for example, the paper on Du-Vote[50] ; the core idea is that neither platform learns the vote, but they each learn information which the server can use to reconstruct the vote. But this involves heavy use of codes that voters have to type, and it is hard to assure usability properties with this kind of system.

Accurate and complete electoral register. As in any election, the starting point is the list of voters who are defined as eligible to vote. Unfortunately, this is often a challenge in industrial ballots. The union may not have accurate records. There is no straightforward way to eliminate duplicates or incorrect registrants. The secrecy of who is a member of the union makes it impossible for the employer to contribute to this effort.

Interference detection e.g. by analytics and audit. In current industrial election practice, an important aspect of the scrutineer's job is to examine the ballots from a forensic perspective.
He or she will look at response patterns, including voting patterns, and compare them with expected or historic data. This may include undertaking spot checks to verify the eligibility of voters. The possibility of this kind of analysis contradicts the requirements of ballot-secrecy and incoercibility, because it requires information about individual voters and their votes. It is considered desirable and necessary in industrial ballots because of the lack of other means of verifying the correctness of the electoral register.

Security of electoral register and other personal information. The union maintains the list of eligible voters, along with other information (such as their address or other contact details, and perhaps specifics of their employment). There is a clear requirement to hold this data securely.

Usability, inclusiveness and enfranchisement. To ensure inclusiveness and enfranchisement, it is vital that everyone that's eligible can participate in the election.
Therefore, voting systems have to be as accessible and easy to use as possible. This may include having special provisions (voting platforms) for disabled voters. Unfortunately, in information systems of all kinds, security always gets in the way of usability, and electronic voting systems are no exception to this phenomenon. Specific challenges to usability arise in the case of electronic voting: the requirements to allow voters to verify their votes can confront them with terms and concepts that they may find difficult to relate to.

Scrutineer independence. In current industrial election practice, the scrutineer plays an essential role by managing the election. This includes distributing the ballots, collecting the results, analysing voting patterns, investigating and adjudicating on any anomalies, and announcing the result. This practice has evolved over decades, and scrutineers have demonstrated themselves capable of undertaking the role. However, it is not clear that they would be as capable in the context of an electronic ballot as they are in the case of a paper-based ballot. Management of electronic ballots, and detection of fraud in an electronic election, require very different skills than their counterparts with paper-based ballots, and current scrutineers may have not had the decades of experience with electronic elections that they have with manual ones. The attack surface for electronic voting is very different from that of paper-based voting. Electronic voting comes with the inherent difficulty of detecting changes to records that happen in a computer compared to changes that happen to boxes of paper ballots. To address this concern, one might argue that it is vital to include requirements of **independent verifiability** of the kinds described above.

[50] Ryan et al. Du-Vote: Remote Electronic Voting with Untrusted Computers.

4 Identification of some eligible systems

We identify and explore four electronic balloting systems which could be used, and analyse them in terms of the requirements identified in the previous section. We will examine underlying technologies, including blockchain.

4.1 Building society elections

Building societies (and other organisations) hold elections to approve choice of directors and director remuneration. These elections are somewhat similar in scale and nature to industrial ballot elections, so looking at the technology they use may be useful. However, it should be noted that the economic impact of industrial ballot elections may be much greater than for building society elections.

Building societies employ proprietary solutions, which differ across the sector. In the description below, we set out a typical arrangement. The building society sets out the issues on which members are invited to vote. Members may vote by post or electronically. Since electronic collection of ballots is more efficient for the society, they encourage electronic submission, for example by promising to donate a small sum of money to a charity for each electronic submission they receive.

The voter receives a voting pack, which contains voting a code that identifies the voter. To preserve the member's ballot secrecy, this code is generated independently of the voter's society account and other identifying information. The voter casts her vote, by first navigating to the web page for the election. Then she types the voter code to authenticate herself, and completes the ballot. The system may give immediate feedback, in order to prevent inadvertently casting an incorrect ballot (for example, inadvertently choosing both of two exclusive options, or failing to chose another option). These completed ballots are recorded in a database.

Staff members within the society can monitor votes as they come in, performing whatever forensic analysis they deem appropriate. Although the voting codes are meant to ensure anonymity, the system is likely to have recorded which voter received which code, which helps carry out this kind of analysis. When the voting period ends, the system outputs the result. In terms of the properties outlined above, building society election systems offer usability and ballot secrecy from third parties. But they do not offer any form of verifiability, and therefore are very dependent on the integrity and competence of the election managers. They do not have any features to resist voter coercion.

4.2 Helios

Helios[51] is the design of an online voting system that is led by Ben Adida (he did a PhD in cryptography at MIT, worked at Mozilla for several years, and now works at an education-focussed technology company called Clever in San Francisco). Helios is an open design, accompanied by open-source software. Various implementations have been used for many online elections, including elections of University officials (for example, in the University of Louvain, Belgium), and professional association elections (for example, the International Association for Cryptologic Research). Its website declares that more than 100,000 votes have been cast using Helios.

Helios offers simple and relatively usable online voting, and has good verifiability properties. More precisely, it allows a voter to verify that her ballot has been included in the tally. The verification process works as follows. Each voter obtains a smart ballot tracker which can be checked against the ballot "tracking center" to ensure that the ballot was received and tallied

[51] Documentation and open-source code is available at https://vote.heliosvoting.org/ . That website also allows one to set up an election and directly invite voters to vote.

appropriately. This means that no one, not even the administrators of the Helios Voting system, can alter a voter's vote. Voters and observers can also verify that the declared outcome corresponds to the tally of the votes actually cast (UV above). This works by using cryptography that, while hiding the actual votes, allows anyone to repeat the calculations necessary to compute the outcome.

Although Helios provides good verifiability properties, it does not attempt to protect voters from coercion. Helios does allow re-voting, and in some circumstances this can offer some protection from coercion. But re-voting in Helios does not offer any protection because of the ability of any observer (and therefore a coercer) to see which votes have been included in the final tally (UV property above). In other words, a coercer can check to see if a coerced voter has re-voted and cancelled the coerced vote, or not. Helios is targeted at low-stake online elections where coercion is not expected to feature prominently. As the designers write: "online elections are appropriate when one does not expect a large attempt at defrauding or coercing voters. For some elections, notably US Federal and State elections, the stakes are too high, and we recommend against capturing votes over the Internet... we don't trust that people's home computers are secure enough to withstand significant attacks."

Helios allows the election manager to see which voters have actually voted at any particular time (but not how they have voted). This allows some kinds of forensic analytics to be carried out. If needed, one could extend Helios to allow the decryption of an individual voter's ballot.

4.3 Estonian system

In 2005 Estonia introduced internet voting as an additional voting channel alongside polling place voting. Between 2005 and 2015 the internet voting system has been used in 8 elections in local municipal elections, parliamentary elections, and European parliamentary elections, most recently in the 2015 general election in which 176,491 internet votes were cast, just over 30% of the total. Estonia does not use postal voting, and remains committed to internet voting. The system is based on the Estonian Digital ID card, which all Estonian citizens are required to have. This is a smart card which contains the citizen's eID, supporting verification of the ID and also digital signing of documents for the ID. There is also mID, a mobile phone version of eID provided through SIM cards with added eID functionality for authentication and digital signature.

The system was designed by Tarvi Martens, Head of Internet Voting at the State Electoral Office of Estonia. It incorporates a number of mechanisms seen in the academic secure e-voting literature for secure electronic voting.

The source code of the system is available for public review[52] , and the approach is briefly explained on an associated website[53].

As part of this review, a team including Sir Ken Knight and Steve Schneider visited Estonia for discussions about the Estonian e-voting system.

Casting a vote - voter experience

We first describe the system from the viewpoint of a voter who wishes to cast her vote electronically, and the steps she needs to go through in order to do this.

● In advance of the election, the voter downloads the Voting application onto her computing device from which she intends to cast her vote

[52] Estonian Internet System Source Code , https://github.com/vvk-ehk/evalimine (last accessed 25/7/17)
[53] http://www.vvk.ee/voting-methods-in-estonia/

● In order to vote, the voter authenticates herself to the system through the voting application, either by means of the Digital eID card, or through mID.

● The system confirms the voter's identity and that the voter is eligible to vote.

● The voting application on the voter's device offers the list of candidates. The voter selects her choice of candidate from the list and confirms her choice to the application.
The voting application casts the vote by submitting the choice to the central voting system servers.

● The voter can also carry out a *cast as intended* verification check. This step is optional and at the preference of the voter: she has the option of verifying that the vote received matches her selection. To do this she uses a *verification application* installed on a second device, for example a mobile phone. Verification consists of scanning a QR code displayed on the screen of the voting application following the casting of the vote, and downloading the vote from the central system. The verification application reveals the vote that was cast, and the voter can verify that this corresponds to her choice.

● The voter has the option to vote multiple times if she wishes. In such circumstances the latest vote submitted is the one accepted as the cast vote. Furthermore if a paper vote is submitted then this is accepted as the cast vote in preference to any electronic vote.

Under the hood

● When the candidate selection is made to create a vote, the Voting Application firstly encrypts the vote to generate a ciphertext, and the ciphertext is then digitally signed to provide assurance to the system that the vote is authentic and to associate it with the voter, since subsequent votes from the same voter mean that this vote will need to be removed from the tally.

● The vote is encrypted with the Electronic Voting System's public key, meaning that the Electronic Voting System secret key is needed to decrypt it. This encryption of the vote ensures that the vote remains secret until the point of decryption, and is the mechanism which provides vote privacy.

● However the device on which the vote was cast knows the vote that was cast, and so a key logger or malware could in principle reveal the vote. Therefore the voter is required to trust that the platform she is using to cast the vote is secure against such threats.

● The verification application is able to reconstruct the ciphertext with the information provided to it in the QR code (a two-dimensional bar code) from the Voting Application, and thereby confirm that the correct candidate was encrypted.

● The digital signature on the encrypted vote provides the assurance to the Electronic Voting System that the vote was provided by the corresponding voter.

● Once all the votes have been received, the processing of the votes is carried out in a universally verifiable way, using established cryptographic mechanisms. This provides *universal verifiability* of the processing of the cast votes. All of these steps can in principle be validated by independent observers.

a. ineligible votes (i.e. those superceded by others) are first removed, resulting in the set of eligible votes;

b. the signatures are removed to yield the set of encrypted votes;

c. Cryptography is used in a procedure (known technically as a *cryptographic mixnet*) to shuffle and anonymise the encrypted votes in a verifiable way (so the encrypted votes at the end match the encrypted votes at the beginning), analogous to shaking a ballot box of paper ballots;

d. and the resulting set of encrypted votes are decrypted to yield the votes;

e. the revealed votes can then be tallied.

Key Properties

The desirable properties for electronic voting systems discussed in Section 3 are addressed by the system in the following ways:

● **Individual verifiability** : voters get a verification code to check that the ciphertext received by the Electronic Voting System is correct, and this is checked on a different platform to the voting platform. The voting platform is unable to change the cast vote without a high chance of detection. The Electronic Voting System is unable to change the vote since the ciphertext is signed by the voter, and tampering would invalidate the signature.

● If the voter does not verify their vote then malware on the voter's device could in principle alter the vote as it is cast. The key defence against this is that the malware does not know whether the voter will verify the vote, so a sufficient number of voters verifying their vote will detect such tampering with very high probability.

● **Eligibility verifiability** : the voter roll is public, and the eID cards provide digital signatures on encrypted votes so the eligibility of the voter to cast the vote can be checked.

● **Universal verifiability** - the use of cryptographic mixnets (a checkable way of shuffling the votes, protected by cryptography) and provable decryption provides verifiability evidence which can be independently checked to establish that the mixing and the decryption have been done correctly

● **Privacy for the encrypted votes** : only the election authorities have the election secret key which provides the means to decrypt the ciphertext. Breach of privacy can be further protected against a single point of failure by splitting the key into several parts held by different parties, such that a threshold of trusted parties must cooperate to do the decryption. Malware or vote logging software on the voting device or verification device could in principle capture and leak the voter's vote, breaching privacy. This would not be detected by the verification checks, since they only check the integrity of the election and not breaches of privacy.

● **Tamper-detection** of the cast votes:
a. since the votes are signed they cannot be altered without detection;
b. votes cannot be added into the system since signatures of legitimate voters are required;
c. removal of a vote from the database is detectable by the voter who has cast a vote that has subsequently been removed;
d. universal verifiability enables detection of any tampering of votes as they are processed and tallied.

● **Coercion-resistance** is provided by allowing multiple votes: if a voter is coerced to vote in a particular way contrary to their preferred choice, then the ability to cast a subsequent vote, and a paper vote, means that they can nullify the coerced vote.

- **Receipt-freeness**: the verification code provided to the voter together with the encrypted vote submitted to the system enables the vote to be reconstructed (this is how the verification app works). However the ability to cast a subsequent vote means that this is not necessarily a receipt of the final vote cast.

Assumptions

- The eID system is trusted to provide assurance of identity of individuals and correct digital signatures.
- There is an assumption that sufficient voters will carry out verification steps to confirm the system is behaving correctly. Checks by a few percent of voters (with no evidence of incorrect behaviour) are sufficient to give a high statistical degree of assurance that the system is behaving correctly with respect to integrity.
- A coercer does not have access to the database of encrypted cast votes. This is required for receipt-freeness and coercion resistance. This means that the independent observers performing universal verification checks must be trusted not to pose a coercive threat.

4.4 CHVote - Internet Voting System from Geneva

Switzerland has a tradition of direct democracy, and cantons typically run 4 referenda per year, resulting in a high level of postal voting (the figure of 95% is quoted[54]). In 2001 internet pilot projects were launched in three cantons including Geneva, leading to the inclusion of internet voting in Federal elections in Geneva from 2011. In 2013 the Swiss Federal Council published its Third Report on Electronic Voting, which included requirements for verifiability and for vote secrecy, and a discussion of security issues and assurances[55].

CHVote is the second generation internet voting system being developed, hosted and operated by the Canton of Geneva. It will replace the system currently in use, with deployment by 2019 planned for the Canton of Geneva and also made available to other cantons. It is currently at an advanced stage of development: its complete technical specification is in the public domain[56], and a proof of concept system i s available as open source[57].

The voting process - voter experience

The voter authenticates herself and confirms her vote through the use of *codes* sent between the voter and the election management system.

- **Prior to an election**, the voter is sent a printed *voting card* which contains the following information:

a. a *voting code* , which is the voter’s credential for submitting a vote;
b. *verification codes* for each choice on the ballot;
c. a *confirmation code,* the voter’s credential for confirming the vote;
d. a *finalisation code* to confirm successful casting of the vote.

[54] Daniel Franke Security Analysis of the Geneva e-voting system , Technical University of Darmstadt, Lecture Notes in Informatics, volume P220, 2013

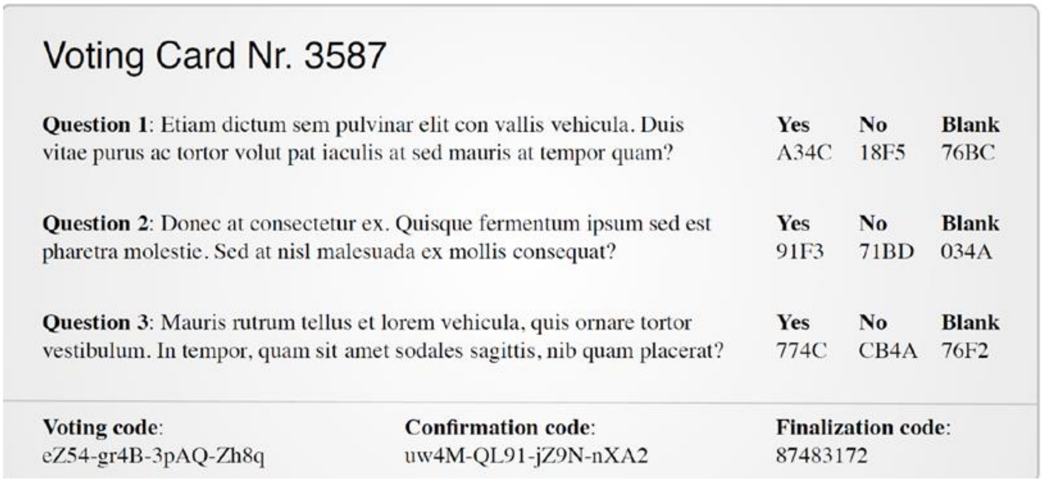
[55] Swiss Federal Council, Ergänzende Dokumentation zum dritten Bericht des Bundesrates zu Vote électronique ,
[Additional documentation on the third report of the Federal Council on Electronic Voting], June, 2013

[56] Rolf Haenni, Reto E. Koenig, Philipp Locher, Eric Dubuis, CHVote System Specification Version 1.0 , Bern University of Applied Sciences, CH-2501 Biel, Switzerland, April 2017.

[57] Republique et Canton de Geneve, CHVote : a public system, Swiss and open source https://republique-et-canton-de-geneve.github.io/chvote-1-0/index-en.html , accessed 15/7/17

● Each voting card is different, so the credential codes and verification codes are unique to each voter. All of this information must be kept confidential to the voter, since it enables her vote to be cast.

The CHVote System Specification Version 1.0 includes the following example of a Voting Card. This card asks for three choices from the voter.



Voting Card Nr. 3587

Question 1: Etiam dictum sem pulvinar elit con vallis vehicula. Duis vitae purus ac tortor volut pat iaculis at sed mauris at tempor quam?	**Yes** A34C	**No** 18F5	**Blank** 76BC
Question 2: Donec at consectetur ex. Quisque fermentum ipsum sed est pharetra molestie. Sed at nisl malesuada ex mollis consequat?	**Yes** 91F3	**No** 71BD	**Blank** 034A
Question 3: Mauris rutrum tellus et lorem vehicula, quis ornare tortor vestibulum. In tempor, quam sit amet sodales sagittis, nib quam placerat?	**Yes** 774C	**No** CB4A	**Blank** 76F2

Voting code: eZ54-gr4B-3pAQ-Zh8q	**Confirmation code**: uw4M-QL91-jZ9N-nXA2	**Finalization code**: 87483172

● **To cast her vote**, the voter uses her device to interact with the election management system.

a. The voter selects her choices from the list presented by the voting client (which should match the list on her voting card). She casts her vote by submitting her choices together with her voting code provided on the voting card. The voting code provides the voter's credential.

b. The system responds by returning the verification codes corresponding to the selected choices.

c. The voter checks that the codes returned from the system indeed match the verification code on her voting card for her selected choices. In this way the voter checks that the vote was *cast as intended.*

d. The voter submits the confirmation code from her voting card to confirm that the verification code was correct. The vote is accepted by the system on receipt of the correct confirmation code.

e. The voter receives the finalisation code from the system. Checking that it matches the finalisation code on the voting card confirms that vote casting has been successful.
The specification of CHVote does not discuss the possibility of repeated voting, since any form of vote updating is prohibited by Swiss election law. However it appears to be possible from a technical point of view.

Under the hood

● Responsibility for running the election is divided across several election authorities so that no single authority needs to be trusted for the secrecy of the election as long as a threshold number can be trusted. The election uses threshold cryptographic keys which require a threshold of authorities to carry out decryption.

● The printing authority is responsible for the secure printing of the voting cards and is therefore a highly trusted component of the election authorities. These cards contain very sensitive information, providing the credentials for a voter to participate in an election, and the confirmation codes for a voter to confirm her vote has been correctly received. If leaked, the information enables anyone to cast a vote for the voter. The voter would observe if a vote has already been cast for her when she attempts to cast a vote, but this would not be picked up if she simply decided not to vote.

- The voting cards are sent to eligible voters. Authentication of a voter is obtained through provision of the voting code contained on the card. The method by which a voting card reaches a voter is therefore a key element of the authentication mechanism, since knowledge of the voting code is taken as evidence of the identity of the voter.

- To vote, the voter interacts with the voting client on her voting device. This might be presented through a web page, or it might be an application downloaded and installed on the device. The voting client interacts with the central election management system to submit voting information and to receive confirmations.

- The voter provides her choices and her voting code to the voting client. The client converts these into an encrypted form and submits to the central election system. The encryption is provided in such a way that the system can check that the voting code has not been used previously (since it should only be used at most once), although the voting code itself is masked within the encryption. This interaction is carried out over an encrypted channel so the content cannot be altered by a third party.

- The system returns the verification codes corresponding to the choices made by the voter. Since no-one other than the election system has possession of the verification codes, receipt of the correct codes confirms to the voter that her choices have indeed reached the election system. No intermediate party can have intercepted and suppressed the vote, since it would not have been able to provide the correct codes.

- Provided that the verification codes are correct, the voter now provides the confirmation code to the voting client on her device. The client cryptographically combines the confirmation code with the choices that were confirmed and submits this combination back to the election system. This provides the election system with confirmation from the voter that her choices match those received, and hence the system can now consider the vote to be submitted.

- Use of the verification codes and confirmation code deals with the danger of malware or a fake client on the voter’s device changing the voter’s vote. In particular, if a vote is altered on the device before submission to the election system then the wrong verification codes will be returned. The malware or fake client does not have the correct verification codes to spoof the voter. The voter will not see the verification codes she is expecting for her choices. Therefore she should not provide the confirmation code in this case, and should instead terminate the attempt to vote and vote via a different channel (e.g. by post). The malware also does not have the confirmation code, so cannot spoof the election system that the voter has confirmed the (incorrect) vote. Therefore the system will not consider that the vote has been cast, and will abandon this interaction as an incomplete attempt to vote.

- After voting has completed, the submitted and confirmed ballots are passed through a re-encryption mixnet managed collectively by the election authorities. This shuffles the encrypted votes and yields an equivalent set of encrypted votes. These are then decrypted to reveal the votes and tally the election. Both of these processes are universally verifiable: independently checkable evidence is published that can be used to confirm that the mixing has taken place correctly, and that the decryption to extract the votes has been done correctly.

Key properties

● **Individual verifiability** is achieved through the exchange of codes. The voter has confirmation that her vote was received by the election system by receiving the correct verification codes. All voters are forced to follow this procedure in order to cast their vote, so individual verifiability is enforced for every voter. This also provides tamper-detection of the vote as it is cast, since any tampering will result in the incorrect codes being returned.

● **Eligibility verifiability** : the election system can check that all votes received correspond to eligible voters who have been issued valid codes. However this cannot be independently checked.

● **Universal verifiability** : given the set of cast votes, the process of producing the tally is universally verifiable since all the steps can be independently checked.

● **Vote privacy:** the choices made by the voter are sent only in encrypted form, and the verification codes do not reveal the choices that were made. Hence the vote is private with respect to an external eavesdropper. However the voter's device learns the vote, so this information will be available to malware. The device must be trusted to be secure with respect to malware and to retain the secrecy of the vote.

● **Coercion resistance:** repeated voting is not permitted in Swiss law so once the vote is cast it is the voter's definitive vote. Hence a voter can be forced to cast their vote in the presence of a coercer. The CHVote system specification notes that this threat is already possible for postal voting, and that the legal ordinance requires only that this risk is not significantly greater.

Assumptions

● The codes on the voting cards are known only by the voter and the election authorities, and in particular are not known by any third parties. This rests on the assumption that the voting cards are distributed to the correct eligible voters, without interception or leakage of their information.

4.5 Blockchain

We end this section with a discussion of blockchain, motivated in part by the existence of quite a lot of excitement and enthusiasm around blockchain in the financial sector, in startups, and in UK Government too[58]. Blockchain is not a voting system like the four that we have 9 considered above, but it has been invoked as possibly contributing to such systems. We look at this idea.

A blockchain is a data structure that is used to maintain a continuously growing list of records or events, periodically grouped together into blocks. By design, blockchains are inherently resistant to modification of the data. Blocks are tied together using cryptographic operations called hashes. Once inserted, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks. The bitcoin cryptocurrency has the blockchain at its foundation; that blockchain contains a record of all the bitcoin transactions ever made.

Because of their resistance to modification, blockchains have been suggested as a means to secure voting. Indeed, blockchains are potentially a useful ingredient to a voting system: a blockchain of all the votes cast so far can be maintained, and the nature of blockchains would make alteration or deletion of votes difficult. However, while blockchains are a useful ingredient, they come with a certain cost and complexity concerning who maintains the blockchain (whether this is done by distributed signers, as in so-called private blockchains, or by a proof-of-work system, as in the global Bitcoin blockchain). There are other ways to secure the

[58] Distributed ledger technology: Blackett review. UK Government Office for Science. 19 January 2016. https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

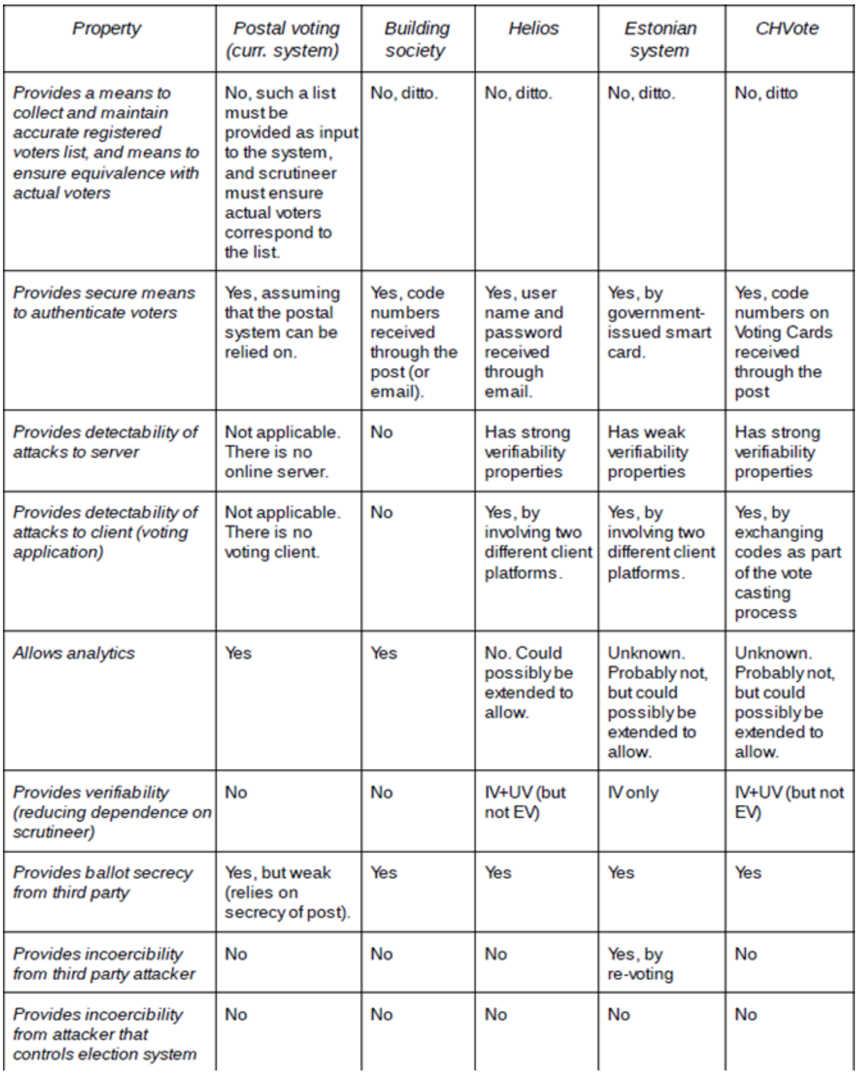
stored votes (for example, the use of verifiability mechanisms that allow any observer to detect modifications), and such methods may be more fit-for-purpose and easier to deploy than blockchain.

Moreover, blockchains only address one security issue in electronic voting, namely, the possible alteration of votes already cast. As we have indicated, there are many other security issues, including the alteration of votes before they are cast, corruptions in the tallying system, and corruptions of the voter register, as well as coercion and privacy attacks. None of these issues are addressed by blockchain. Indeed, the necessarily open nature of blockchains can make some issues, such as voter privacy, more difficult to achieve.
Thus, while blockchain technology can be a useful ingredient to secure one aspect of voting, it is certainly not a complete solution, and may in fact introduce more complications than it solves.

5 Analysis of delivered properties

All of the systems we have examined are real systems that have been used in real elections, and therefore all of them have been engineered to offer good usability properties. However, it can readily be seen that, as always, security conflicts with usability. The system with the least security (building society elections) is the most straightforward from the voter's point of view.
Helios has better security properties, because it offers voters the opportunity to directly check that their vote is included, and it offers any observer the option to check the tally computation.
This introduces some usability challenges; the voter has to understand what auditing a ballot means, and the voter necessarily sees some strings of numbers and letters which represent encrypted votes. The Estonian system is in this respect similar to Helios: it offers some verifiability properties, and therefore similar usability issues to those of Helios are present there. But the Estonian system aims to address the question of voter coercion, which Helios does not. To address this question, the Estonian system allows re-voting. A coercer is not able to see whether a vote got cancelled by a re-vote or not, and therefore in this case re-voting can be an effective way to address coercion. Helios also allows re-voting, but because Helios offers UV, a coercer can see if a vote got cancelled by a re-vote, and therefore re-voting in Helios does not address coercion.

Whether a given property holds depends on whether an attacker can control the election servers or not. For example, the Estonian system is receipt-free in the case that the coercer can't control the servers, but merely has the information given to him by the voter. But it is not receipt-free if the coercer controls the voting server and can access all the ciphertexts. A recapitulation of these issues is given in the following table.



Property	*Postal voting (curr. system)*	*Building society*	*Helios*	*Estonian system*	*CHVote*
Provides a means to collect and maintain accurate registered voters list, and means to ensure equivalence with actual voters	No, such a list must be provided as input to the system, and scrutineer must ensure actual voters correspond to the list.	No, ditto.	No, ditto.	No, ditto.	No, ditto
Provides secure means to authenticate voters	Yes, assuming that the postal system can be relied on.	Yes, code numbers received through the post (or email).	Yes, user name and password received through email.	Yes, by government-issued smart card.	Yes, code numbers on Voting Cards received through the post
Provides detectability of attacks to server	Not applicable. There is no online server.	No	Has strong verifiability properties	Has weak verifiability properties	Has strong verifiability properties
Provides detectability of attacks to client (voting application)	Not applicable. There is no voting client.	No	Yes, by involving two different client platforms.	Yes, by involving two different client platforms.	Yes, by exchanging codes as part of the vote casting process
Allows analytics	Yes	Yes	No. Could possibly be extended to allow.	Unknown. Probably not, but could possibly be extended to allow.	Unknown. Probably not, but could possibly be extended to allow.
Provides verifiability (reducing dependence on scrutineer)	No	No	IV+UV (but not EV)	IV only	IV+UV (but not EV)
Provides ballot secrecy from third party	Yes, but weak (relies on secrecy of post).	Yes	Yes	Yes	Yes
Provides incoercibility from third party attacker	No	No	No	Yes, by re-voting	No
Provides incoercibility from attacker that controls election system	No	No	No	No	No

An important comparison one might make of each of the systems is the security comparison with current postal-ballot practice. In all four cases, the electronic voting system dramatically changes the nature of the threat landscape. Threats to postal balloting might focus on interference with the communication channel (the post). There might also be threats involving voter coercion, and perhaps less plausibly, insider attacks on the scrutineer’s processes. In the case of electronic balloting, interference with the electronic communication channel is much less likely, because the communications are encrypted; and the threat of interference with material through the post remains about the same. However, attacks on the scrutineer’s process become more likely, because they can potentially be done remotely without requiring the collusion of any insiders. In addition, a new threat arises, namely, attacks on the voter’s platform (phone or laptop). The threat of coercion remains about the same.

6 Conclusions

The main contribution of this document is to identify some criteria along which voting systems may be judged, and to introduce four systems which could be considered as the basis for electronic industrial ballots. All four systems have been used in real elections[59] . In the case of building society elections and Helios, the elections were of relatively small scale and relatively low national importance. In the case of the Estonian system and in Switzerland, the elections were larger scale political elections and national importance. In conducting this review, we have made some observations which seem particularly pertinent to the question of whether suitable technology exists for industrial ballots. We recall those observations now.

● There are some countries that are using internet-based voting for political elections of national importance (such as Estonia and Switzerland). But there is also much opposition to doing that, from academics and journalists alike. Such opposition is based on the opinion that none of the systems we have created have adequate security properties (see table).

● Industrial ballots are generally of smaller scale and smaller national importance than parliamentary elections or (in other countries) presidential elections. This means that they represent a smaller attack target, and therefore the cyber security threat is correspondingly smaller, than it would be for larger, national elections. Nevertheless, large industrial ballots could have substantial impact on the economic well-being of the UK, and therefore attacks on those could be of interest to state-sponsored adversaries or to organised criminals.

● One cannot eliminate the possibility of undetected interference in an electronic balloting, but one cannot eliminate that possibility in a present-day postal balloting either. For a small-scale election, the difficulty an attacker has in achieving undetected interference is considered about the same for electronic and postal elections. However, for a large-scale election, the difficulty an attacker has in achieving undetected interference is less in an electronic ballot than in a postal ballot. Verifiability provides some mitigation against this threat.

● One also cannot eliminate the possibility of disruption of an election by means of denial-of-service attacks. This may result in a balloting period having to be extended, or even postponed.

● If one is to contemplate using internet balloting for industrial ballots, the following considerations should be borne in mind.

○ It would make sense to start with smaller elections (for example, those involving a few hundred voters), rather than large ones (tens of thousands of voters).

○ Scrutineers should be required to demonstrate cyber security competence when they are approved as scrutineers.

○ Systems should be sourced from competent organisations able to demonstrate adherence to the highest cyber security standards.

○ Election systems that offer verifiability properties so that voters, observers and scrutineers can independently verify aspects of the election should be preferred.

[59] In the case of CHVote an earlier version has been used

Author biographies

Mark Ryan is Professor of Cyber Security at the University of Birmingham, where he leads the *Security and Privacy* research group (consisting of 10 academics and 15 other researchers). He is the holder of the *HP* (formerly Hewlett Packard) *Research Chair in Cyber Security* at Birmingham (2016-2021). Prior to that, he was EPSRC Leadership Fellow (2010-2015), a prestigious award given through a competitive process. He has held about £2.5M in research funding, including two large projects (*Trustworthy Voting Systems* and *Analysing Security and Privacy Properties*) which directly relate to the subject matter of this proposal.

Relevant publications:
Gurchetan S. Grewal, Mark D. Ryan, Liqun Chen and Michael R. Clarkson. Du-Vote: Remote Electronic Voting with Untrusted Computers . In 28th IEEE Computer Security Foundations Symposium (CSF), 2015.
Gurchetan S. Grewal, Mark D. Ryan, Sergiu Bursuc and Peter Y. A. Ryan. Caveat Coercitor: coercion-evidence in electronic voting. In IEEE Symposium on Security and Privacy, 2013.
Myrto Arapinis, Veronique Cortier, Steve Kremer, Mark Ryan. Practical Everlasting Privacy. In Principles of Security and Trust, 2013.
Sergiu Bursuc, Gurchetan Grewal and Mark Ryan. Trivitas: Voters Directly Verifying Votes. In VoteID, 2011.

Steve Schneider is Professor of Computer Security at Surrey University. He leads the Surrey Centre for Cyber Security. He has been working in verifiable electronic voting research for over a decade, including leading the Surrey contribution to an EPSRC-funded research project “Trustworthy Voting Systems” 2009-2014 (in which Mark Ryan, Birmingham was also involved).
He led the team that developed the vVote verifiable voting system used in the 2014 State Election in Victoria, Australia. The system integrated with the front end and election management system developed by the Victorian Electoral Commission. It was made available to vision and motor impaired voters, those with languages other than English, and voters in London voting over the internet from Australia House.
He was general chair of the International Conference VOTE-ID held in 2013 at the University of Surrey, and was a keynote speaker at the 2015 version of the conference held in Berne.

Relevant publications:
Craig Burton, Chris Culnane, Steve Schneider: vVote: Verifiable Electronic Voting in Practice . IEEE Security & Privacy 14(4): 64-73 (2016)
Murat Moran, James Heather, Steve Schneider: Automated anonymity verification of the ThreeBallot and VAV voting systems . Software and System Modeling 15(4): 1049-1062 (2016)
Peter Y. A. Ryan, Steve Schneider, Vanessa Teague: End-to-End Verifiability in Voting Systems, from Theory to Practice . IEEE Security & Privacy 13(3): 59-62 (2015)
Chris Culnane, Peter Y. A. Ryan, Steve Schneider, Vanessa Teague: vVote: A Verifiable Voting System . ACM Trans. Inf. Syst. Secur. 18(1): 3:1-3:30 (2015) [i4]
Morgan Llewellyn, Steve Schneider, Zhe Xia, Chris Culnane, James Heather, Peter Y. A. Ryan, Sriramkrishnan Srinivasan: Testing Voters' Understanding of a Security Mechanism Used in Verifiable Voting . EVT/WOTE 2013
Sébastien Foulle, Steve Schneider, Jacques Traoré & Zhe Xia, Threat analysis of a practical voting scheme with receipts , VOTE-ID 2007
David Chaum, Peter Y. A. Ryan & Steve Schneider, A practical voter verifiable election scheme , ESORICS 2005, Springer LNCS.

This publication is available from www.gov.uk/beis

Contact us if you have any enquiries about this publication, including requests for alternative formats, at:

Department for Business, Energy and Industrial Strategy
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

Email: enquiries@beis.gov.uk