GRESHAM COLLEGE

13 February 2018

SHOULD WE VOTE ONLINE?

PROFESSOR MARTYN THOMAS

Introduction

Democracy depends on elections and the legitimacy of a democratically elected government is strengthened if a high percentage of those eligible to vote actually cast a ballot and if the electoral process is seen to be free and fair. It is important that the losers in an election can have confidence that their losing was not the result of a flawed or corrupt system for registering voters or recording and counting their votes. This is especially important in very close or highly polarised ballots.

In the UK, most citizens aged over 18 are entitled to vote in parliamentary elections if they have registered to do so[i]. these people, the UK electorate, number about 47 million[ii]. The rules differ between parliamentary elections and those for Local Government; for the European Parliament; for the Scottish Parliament; for the Northern Ireland Assembly; for the National Assembly for Wales,; for Local Mayors; for Mayor of London and London Assembly; for Police and Crime Commissioners and for Referenda[iii]. This complexity would need to be taken into account in any online voting system and may increase the risk of software errors but I shall ignore it in the discussion of basic principles that follows.

In UK parliamentary elections, about 89% of those eligible to register have actually registered correctly; about 68% of those registered to vote actually did so in the latest parliamentary election. Participation is far lower than this in local elections.

Many countries use forms of electronic voting to improve the administration of elections and to shorten the time taken to count the votes and to announce results. The most commonly used form of electronic voting involves touch screens in private booths in polling stations or other locations rather than online voting using the voter's mobile phone, pc or other electronic device.

Such online consumer devices are increasingly widely used for banking and to interact with many Government services; they are also used for opinion surveys and for the election of officers and other votes in many organisations. So should Parliamentary and Local Government elections give voters the option of voting online? It has been suggested that this would greatly increase participation in elections but this does not appear to be supported by the available evidence.

This lecture explores the issues and describes what has happened when on-line voting has been used, and considers on-line voting in the context of the strengths and weaknesses of the UK electoral systems.

The Current (2018) UK Voting System

Registration

A citizen can register to vote when they are:

- 16 years old in England, Wales and Northern Ireland (and vote when they are 18)
- 14 years old in Scotland (and vote in Scottish elections when they are 16 and other elections when they are 18)

Voting in person

Anyone who has registered to vote can vote in person at a Polling Station in the relevant constituency.

Postal voting

Anyone can apply to vote by post. The great strength of the postal vote is that it is simple to use; most people are familiar with the process and it requires very little effort to understand how it works. On the negative side, it has been argued that it is not sufficiently secure. For instance in a particular case related to the 2004 Birmingham city council elections, the election commissioner said "The ease of postal vote fraud and the difficulty of policing it led to such a great upsurge in personation that, in the Birmingham case, the number of false votes was virtually half of all votes recorded as having been cast for the winning candidates."[iv] . He heard evidence that thousands of postal votes had been stolen and said that the scale of fraud would disgrace a "banana republic". Postal voting fraud appears to be quite widespread: frauds have been detected in several UK elections, in different constituencies and by supporters of different political parties.

Proxy voting

It is also possible to vote by proxy. People who are unable to vote by other means can nominate another person to vote on their behalf - as long as they are registered to vote and they are allowed to vote in the same type of election. A proxy can act for several people if they are all close relatives.[v]

The properties of a good voting system

The principles that underpin democratic elections have been set out by the Council of Europe through the European Commission for Democracy through Law (known as the Venice Commission). Their code of good practice[vi] says that the five principles underlying Europe's electoral heritage are that voting should be *universal, equal, free, secret and direct*. These principles are expanded and explained in the code. Article 3 of the Additional Protocol to the European Convention on Human Rights also explicitly provides for the right to periodic elections by free and secret elections[vii].

Of the five principles, *free* and *secret* have most relevance to online voting. This is what the code of good practice states about *freedom*:

(paragraph 3.2) **Freedom of voters to express their wishes and action to combat electoral fraud**

> *i. voting procedures must be simple;*
>
> *ii. voters should always have the possibility of voting in a polling station. Other means of voting are acceptable under the following conditions:*

iii. postal voting should be allowed only where the postal service is safe and reliable; … fraud and intimidation must not be possible;

iv. electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent;

… … and this is what they say about *secrecy:*

(paragraph 4) **Secret suffrage**

a. For the voter, secrecy of voting is not only a right but also a duty, non-compliance with which must be punishable by disqualification of any ballot paper whose content is disclosed.

b. Voting must be individual. Family voting and any other form of control by one voter over the vote of another must be prohibited.

c. The list of persons actually voting should not be published[viii].

d. The violation of secret suffrage should be sanctioned[ix].

As we shall see, it is difficult to devise an online voting system that respects all these principles. Indeed, many expert computer scientists believe that it is impossible to devise a system that is simultaneously secure, verifiable and secret.

The secret ballot has been the cornerstone of voting in the UK since 1872. The current scheme was designed to protect against influence and corruption, by reducing their efficacy, whilst retaining the ability to trace particular ballot papers at court proceedings to combat fraud. This is done through the corresponding number list (on which polling station staff record the number of the issued ballot paper against the elector's number). This system is therefore not completely secret although there are legal penalties if polling station staff or anyone else abuses the system. The Law Commissioners have proposed that the law should be be brought up to date and extended to cover postal voting[x].

The Risks and Threats to a Fair Election

From these principles, we can see that there are many possible ways in which a fair election might be compromised. Here are some of them.

A. Non-existent or ineligible people may be fraudulently registered as voters or the registration of an eligible voter may be directed to the wrong person.
B. Some (groups of) people who are entitled to vote may be wrongly denied a vote.
C. Votes may be stolen by impersonating a registered voter.
D. Voters may be coerced to vote in a way that they would not have chosen without coercion.
E. Voters may agree to sell their vote.
F. The secrecy of the ballot may be violated, revealing how individual voters voted.

G. A denial of service (DoS) attack may prevent votes being cast by a particular group of voters or by enough voters to cast doubt on the legitimacy of the result.
H. The system may not record or count votes correctly, leading to an incorrect result.
I. A cyberattack may change the counting of votes or enough individual votes to affect the election result.
J. The system may lose the trust of voters, leading to loss of confidence in the election result.

A report by the US National Academies, titled **Asking the Right Questions About Electronic Voting**[xi] said

> *The committee also believes that trusted election processes should be regarded as the gold standard of election administration, where a trusted election process is one that works, can be shown to have worked after the election has been held, can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and can be shown to reflect the intent of the voters. … trusted election processes increase the likelihood that elections will be regarded as fair, even by the losing side and even in a partisan political environment.*

Electronic Voting in UK Elections (including on-line)

In English local elections in May 2007 over 1.5 million people in 18 local council areas were able to take part in voting trials by text message, internet, electronic kiosk and via digital TV.

Research for The Electoral Commission had shown there was significant demand for electronic voting and that it might help stem the declining turnout at elections. In an earlier survey more than half (55%) of English adults said that being offered e-voting in some form would encourage them to vote at the next local election. And the youngest group - 18-24 year olds - were most keen to try the new methods with three-quarters saying that e-voting would encourage them to participate. Voting via the internet was seen as most likely to encourage participation (41%) followed by text messaging (33%), electronic kiosks (30%) and digital TV (26%)[xii].

The Electoral Commission reported on these trials (and others)[xiii], saying about electronic voting

> *The May 2007 elections also saw five local authorities (Rushmoor Borough Council, Sheffield City Council, Shrewsbury & Atcham Borough Council, South Bucks District Council and Swindon Borough Council) pilot a range of e-voting solutions, including remote internet voting, telephone voting and the provision of electronic polling stations enabling a 'vote anywhere' environment on polling day. The use of remote e-voting channels required, as an additional security measure, pre-registration by electors and in three of the four pilot schemes (Sheffield, Shrewsbury & Atcham and Swindon) this is likely to have contributed to a significantly lower proportion of electors opting for e-voting channels compared with 2003. In broad terms, the remote e-voting elements of the May 2007 pilot schemes proved successful and facilitated voting, although there were some issues concerning accessibility, public understanding of the pre-registration process and, in at least one pilot area, technical problems in relation to telephone voting. Electronic polling stations in Swindon proved more problematic, with many experiencing connectivity and application issues on polling day. However, in common with the e-counting pilots, there was insufficient time available to implement and plan the pilots, and the quality assurance and testing was undertaken too late and lacked sufficient depth. The level of implementation and security risk involved was significant and unacceptable. There remain issues with the security and transparency of the solutions and the capacity of the local authorities to maintain control over the elections.*

The Commission recommended that no further e-voting is undertaken until the following four elements were in place:

1. *There must be a comprehensive electoral modernisation strategy outlining how transparency, public trust and cost effectiveness can be achieved.*
2. *A central process must be implemented to ensure that sufficiently secure and transparent e-voting solutions that have been tested and approved can be selected by local authorities.*
3. *Sufficient time must be allocated for planning e-voting pilots.*
4. *Individual registration must be implemented.*

The Commission cannot support any further e-voting in the absence of a framework incorporating these recommendations.

Electronic voting in Voting Booths and Electronic Counting

Electronic voting in voting booths is quite widely used internationally, as is electronic counting of votes. This has the potential to greatly reduce the administrative effort required to distribute, collect and count paper ballots and to speed up the count.

The processes are controversial because the accuracy and security of the systems is difficult to verify and because the candidates are unable to supervise the counting process as they can with a paper ballot.

In the UK, the appointed Returning Officer has the authority to allow electronic voting and counting for some elections, though this is uncommon. The Law Commissioners have recommended that the law is made consistent and that it should clearly state what degree of verification and supervision is required.

The issues raised by the technologies available for use in all forms of electronic voting are described in the 160 page report[xiv] from the US National Academies referenced earlier. Reading this report is strongly recommended to anyone who is interested in the technology and practical details.

Recent UK Consultations and Reports on Electoral Reform

In December 2014 The Law Commissions of England and Wales, Scotland, and Northern Ireland jointly consulted on electoral reform. They published an Interim Report[xv] in February 2016. They did not consult on, nor make any recommendations about, voting online. Their recommendations require primary and secondary legislation and the UK Government had not replied to their interim report at the time this lecture was being written.

In January 2015, the Speaker of the House of Commons launched the report of his Commission on Digital Democracy[xvi]. Chapter 10 is on voting and section 10.2 specifically addresses online voting. The Commission said

> *Many of the people we spoke to did not understand why they could not vote online, particularly young people. People are used to doing their banking and other day-to-day activities online and many feel that they should also be able to vote in this way. Some people said that the inconvenience of having to vote in person was off-putting and suggested that online voting would help to increase voter turnout. However, others said that there was little evidence of this.*

The Commission had been told that security was a particular concern:

Some people highlighted concerns about the security of online voting and the potential for cyber-attacks and hacking. Others raised concerns about voter intimidation and vote selling. The Open Rights Group neatly summed up the concerns over the security of online voting:

> *"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."*

The Commission agreed that there is a substantial appetite for online voting in the UK, particularly among young people, saying that it will become increasingly more difficult to persuade younger voters to vote using traditional methods. They concluded that it is only a matter of time before online voting is a reality, but that the concerns about security must be overcome first.

> *Once this is achieved, there will be an urgent need to provide citizens with access to online voting, and the UK must be prepared for this. The Electoral Commission has called on the Government to introduce a "comprehensive electoral modernisation strategy [...] setting out how the wider use of technology in elections will ensure the achievement of transparency, public trust and cost effectiveness". The new online registration system could be a cornerstone of a future online voting system, although it would not solve the problem of verifying the identity of people when casting their vote online. We support the draft recommendation of the Political and Constitutional Reform Committee on Voter Engagement in the UK, urging the introduction of online voting by 2020. We agree that this would make voting significantly more accessible. However, we also agree that concerns about electoral fraud and secrecy of the ballot would need to be addressed first.*

They therefore recommended that …

> *in the 2020 general election, secure online voting should be an option for all voters*[xvii].

… although they did not say how they believed that the concerns about security could be overcome by then.
The UK Government remains committed to implement online voting although (as we shall see later) the National Cybersecurity Centre has said that it is a good thing that there are no current plans to introduce it.
The Scotland Act 2016 gave the Scottish Parliament and Government new powers and responsibilities relating to elections to the Scottish Parliament. These complement their existing responsibilities for local government elections. Towards the end of 2017 the Sottish Government launched a consultation[xviii] on electoral reform that included questions about electronic voting, both online and in polling stations or elsewhere. Their introduction to online voting said:

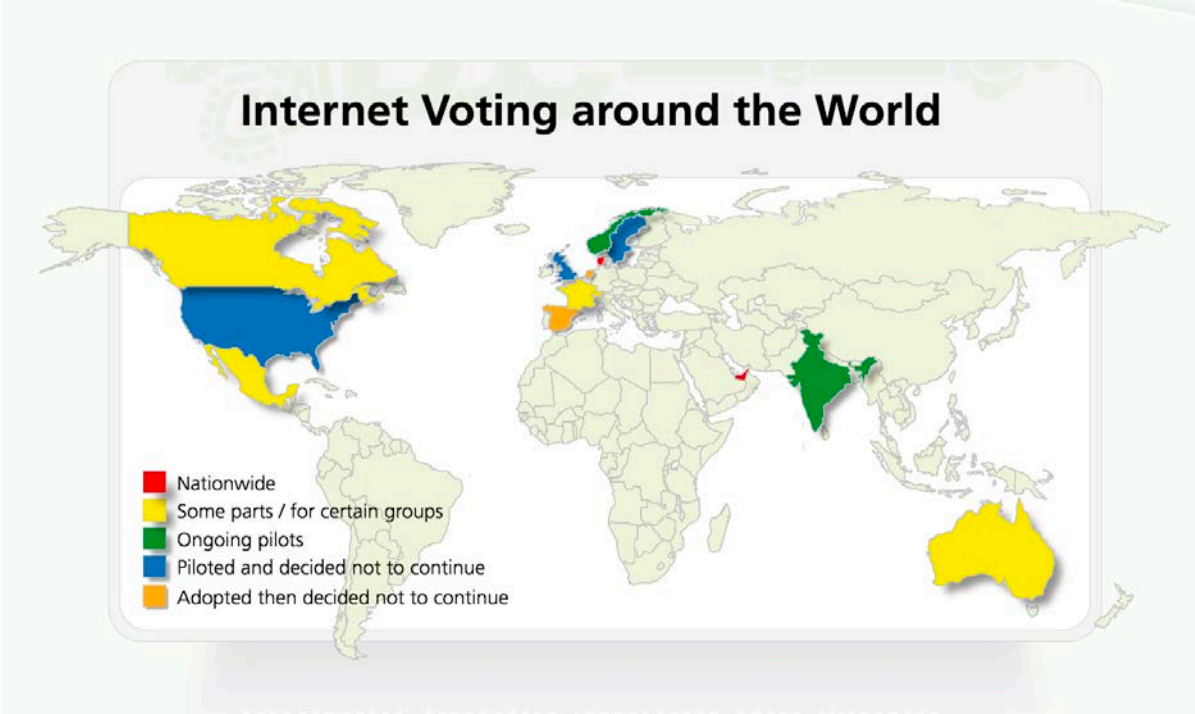
- Internet or online voting would mean voters could cast their vote from a PC, laptop or mobile phone.
- This type of voting is used in Scotland already for some community council and other elections, e.g. trade unions and boards of various bodies.
- However, worldwide it is still relatively uncommon for local or national government elections, though around 15 countries worldwide have, or have trialled, internet voting. The most successful example is Estonia.

- Typically, internet voting systems require voters to register in advance in order to be able to vote online. In addition, for security reasons, the voter might be asked to specify the device e.g. PC, laptop or mobile phone they will use for voting. It would be possible for the voter to change this.
- Typically, once polls are open, the voter receives a message inviting them to vote using a special secure link and security information they were provided with on registration.
- Internet voting could be more convenient for many voters and would potentially allow polls to be "open" for a longer period. Countries such as Estonia allow voters to cast their votes over a period of 7 days, though internet polls close 4 days prior to Election Day.
- Ensuring the security of internet voting and public confidence in it would be extremely important.

The consultation then asked whether people would use online voting, whether it would make them more likely to vote, and whether they wanted to be able to vote on more than one day, and for any other comments. At the time of this lecture the consultation is still open.

The Welsh Government has also announced trials of online voting, electronic counting and remote polling booths in supermarkets.[xix]

Online Voting in Other Countries[xx]



By the end of 2017, 14 countries had used internet voting for binding political elections or referendums, but Estonia was the only one to have introduced permanent national internet voting. Estonian citizens have identity smart-cards that contain cryptography capabilities. With the use of card readers and client software, Estonians can identify themselves to websites and make legally binding signatures on documents. The cards are widely used for online banking. In the online voting system, voters use their ID cards to identify themselves to the server and to sign their ballots.

A group of international experts were invited to observe Estonia's 2013 municipal elections; they witnessed the operation of the voting system's servers, they had meetings with election officials and with the voting software developers in Tallinn and Tartu, they closely reviewed published artefacts from the election including the server source code, written procedures, and nearly 20 hours of official videos that recorded the voting system configuration, administration, and counting processes. Their report[xxi] is detailed and authoritative. The authors commend the effort that has gone into protecting the election system but based on their tests and analyses they conclude that a state-level attacker, sophisticated criminal, or dishonest insider could defeat both the technological and procedural controls in order to manipulate election outcomes, and that short of this, there are abundant ways that such an attacker could disrupt the voting process or cast doubt on the legitimacy of results. Until there are fundamental advances in computer security, they do not believe the voting system can be made safe.

One surprising observation from UK and international experience is that online voting does not appear to increase significantly the proportion of eligible voters who actually vote in elections[xxii] [xxiii] [xxiv] [xxv].

The opportunities for fraud in online voting are different in both nature and scale and international experience of online voting fraud differs. According to a paper by Fairweather and Rogerson[xxvi] use of online voting in the 2000 Arizona Democratic Primary seems to have been successful, at the other extreme an online referendum in the Netherlands had to be abandoned because of fraud – but with our experience of how cyberattacks have developed in recent years we can be confident that those wishing to commit fraud will become more sophisticated in their methods and that those defending the integrity of elections will have to keep investing in new methods of detection, deterrence and resilience.

The Required Properties of an Online Voting System

As we have seen, there has been much discussion of online voting and widespread acknowledgement that the security and integrity of ballots is fundamental to democracy, but little detail on what this would mean in practice. I therefore offer for discussion the following set of properties that an online voting system should have, with some explanations and some comments about the implications.

1. It should be very difficult to register fake voters (and yet easy to register genuine voters).

In the UK, citizens can register to vote either by filling in a registration form or by using an online system[xxvii]. All you need is your name, address, date of birth and National Insurance number.

In 2013 the Electoral Commission reviewed[xxviii] the risk of electoral fraud and reported[xxix]. Individual voter registration was seen as an adequate assurance for the registration process. There seems to be no evidence of any significant degree of fraudulent registration.

2. The system should authenticate that the voter is registered to vote in this election.

The system needs a way to check that the person who is actually voting has the right to do so. In its simplest form, this involves some way of checking that the person who is voting is the same person who registered to vote. This would need to be done with high assurance and without introducing vulnerability to fraud or vote stealing.

The Electoral Commission has proposed[xxx] that voters should be required to present photo ID when voting in person at a polling station. They have suggested that the requirement to quote National Insurance numbers on postal voting forms might reduce the amount of postal voting fraud.

It is likely that any on-line voting system would use Gov.UK Verify[xxxi]. If a voter is permitted to have the assistance of another person to help them to vote (for example because of a disability) this will add further complications.

3. No voter should be able to cast more valid votes than any other voter.

In the simple case, the system should prevent a voter voting more than once. Alternatively, the voter should be permitted to vote several times but only their final vote should be counted. This may be a useful protection against votes being coerced or sold, because the voter could overwrite a coerced or sold vote and thereby make the previous vote of no value.

4. The voter should be able to check that their vote has been recorded correctly.

This is important to give voters confidence in the system but very hard to implement because a compromised system can present compromised evidence.

5. It should be possible to carry out an independent check that all valid votes have been counted and that the totals for each candidate are correct.

Re-counts are quite common where the winning margin in a ballot result is small. When paper voting slips are used, the count can be repeated (manually and independently if necessary) even if the first count used some electronic counting technology. In the case of online voting, it is not apparent that any form of recount would be helpful, because there is limited (if any) scope for an independent system and if the recount differed by even one vote from the original count it would cast doubt on the integrity of the entire online ballot.

How such audits can be carried out has been the subject of much academic research and commentary[xxxii].

6. It should not be possible to discover how a voter voted.

This is fundamental to the secret ballot. As explained earlier, the current paper ballot process includes the "corresponding number system" to allow a court to investigate a claim of fraud, with legal sanctions if the system is abused. Different mechanisms would need to be invented to combat the different threats of fraud that online voting would introduce.

7. It should not be possible to discover whether or not an identifiable voter voted.

In some foreseeable circumstances, abstention in a ballot may be a significant political statement. In designing online voting system, it will be necessary to decide whether or not this is a necessary requirement.

8. There should be defences against coercion and vote selling.

If voters are able to vote online at home, then there is likely to be more coercion and 'family voting', where a dominant member of the household directs how the other members will cast their vote. It also increases the

opportunity for political party activists to visit voters at home and to persuade them to vote for a particular candidate before they leave. These abuses are equally possible with postal voting and there have been serious cases of this in the past. Voting in person, in the privacy of a voting booth, remains the best safeguard. An online system that allows a voter to vote more than once and that only counts the final vote would provide some defence against coercion, because the voter could change their coerced vote later if they wished to do so.

9. The system should be secure against all forms of cyberattack.

Nation states have frequently sought to interfere in other countries' elections, so this must be viewed as a serious threat. Most recently, evidence prepared by Facebook for the US Senate Judiciary Committee said that 120 fake Russian-backed pages created 80,000 posts that were received by 29 million Americans directly, but reached a much bigger audience by users sharing, liking and following the posts. Twitter said that they had identified 50,248 Twitter accounts engaged in what it believed to be automated, election-related activity originating out of Russia[xxxiii]. Many of these Russian accounts also posted messages aimed at influencing the UK Brexit referendum.

> *Russian Twitter accounts posted almost 45,000 messages about Brexit in the 48 hours around last year's referendum in an attempt to sow discord during the vote on whether to leave the European Union, the Times newspaper reported*[xxxiv].

Cyberattack is classified as a top level (Tier One) threat on the UK National Risk Assessment. Last month (January 2018) Ciaran Martin, the head of the UK's National Cyber Security Centre warned in a Guardian newspaper report that a major cyber-attack on the UK is a matter of "when, not if", raising the prospect of devastating disruption to British elections and critical infrastructure[xxxv]. The Guardian added *Cyber-attacks appear to have made electronic voting less likely in the near future. "With the current state of high alert around elections, I think it make sense that there are not any current plans to move to electronic voting," Martin said.*

Despite this, the Welsh and Scottish governments have announced consultations and trials, as I have stated and referenced earlier.

Cyberattacks could be used in many ways: they could influence opinion, disrupt voter registration, disrupt voting, or undermine public confidence in the fairness of the result. The attacks could target individual candidates or constituencies, particular religious or ethnic groups of voters, or the entire election and could range from fake news stories and DDoS (distributed denial of service) attacks to penetration and compromise of online voting software and electronic counting.

Discussion

In deciding whether or not we should vote online, the first question should be *what are we trying to achieve?* There are several possible objectives; the Scottish Government consultation identified five: to increase voter participation; to provide voters with choice and flexibility over how they vote; to reduce the costs of elections; to support the rotation of candidates' names on ballot papers[xxxvi]; and to reduce the number of rejected ballot papers.

Other possible objectives include increasing the proportion of younger citizens who vote, and speeding up the count so that the result can be announced sooner.

A literature search may show whether or not online voting does actually deliver the chosen objectives. As we have seen above, it appears not to increase voter participation, for example. If the evidence is inconclusive it may be necessary to conduct some limited trials. Whether or not online voting would reduce costs is also questionable: on the plus side it might reduce the costs of printing, paper and postage but the computer system costs would be significant (and recurring) and it would still be necessary to offer the means of voting that currently exist.

Then the possible disadvantages should be considered. These include:

- whether it matters that the demographic distribution of internet users is very different from the overall electorate;
- whether error, fraud, coercion and vote selling are made more or less likely;
- whether losing candidates and the electorate in general will have sufficient trust that the election result is fair;
- whether online votes are more or less likely to be the result of considered thought or whether elections might become treated with as little thought as a vote in a reality TV show or a review on TripAdvisor – and whether we think that matters for democracy;
- what the costs and timescales would be for developing and introducing any new computer-based systems – and whether there is a better way to use that money to meet the overall objectives or other priorities.

The paper-based voting system in the UK has significant weaknesses; the postal voting system in particular has attracted scathing criticism – yet it remains in place and is seems to be considered to be good enough. It may be argued that online voting only needs to be better than the existing flawed system to be worth considering. But if you can carry out fraud online you can do it at a much greater scale than would be possible with voting by post, by proxy or in person.

Then there is the matter of security. Every report and consultation agrees that the security issue is very important and must be solved before online voting is introduced but none of them provide a credible solution. The advice from the head of the National Cybersecurity Centre appears to be that we should not vote online or, at least, not yet.

The consensus view of computer scientists is that online voting is a much harder security problem than online banking or online tax returns for the reasons summarised by the Open Rights Group (cited above):

> *"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."*

In this and other areas of society, there seems to be irresistible pressure to adopt digital technologies before the true costs, benefits and unintended consequences have been evaluated. The adoption of online voting will be a political decision—probably influenced excessively by which party is expected to be the beneficiary—but also a decision for us, the electorate. What do we think? **Should we vote online?**

Acknowledgements

I am grateful to Peter Ladkin, Jason Kitcat, Stephen Murdoch, Nicholas Bohm, Ross Anderson, Valerie Shrimplin and Wendy Grossman for their insights and helpful references. Any errors, of course, are mine.

[i] Certain people are excluded from voting. These are: Members of the House of the Lords, convicted persons detained in pursuance of their sentences, and anyone found guilty within the previous five years of corrupt or illegal practices in connection with an election.
[ii] https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/electoral-registration-at-the-uk-general-election-2017/2-the-size-of-the-electoral-register
[iii] https://www.gov.uk/elections-in-the-uk
[iv] http://www.telegraph.co.uk/news/uknews/law-and-order/11560017/Postal-voting-fraud-is- easy-electoral-commissioner-says.html
[v] https://www.gov.uk/apply-vote-proxy
[vi] http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e
[vii] Article 3, Right to free elections: "The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature"
[viii] This is because abstention can be a political choice.
[ix] "Sanctioned" with its original, legal and ethical meaning of "punished".
[x] https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2016/02/electoral_law_interim_report.pdf Chapter 5.
[xi] https://www.nap.edu/catalog/11449/asking-the-right-questions-about-electronic-voting
[xii] https://www.electoralcommission.org.uk/i-am-a/journalist/electoral-commission-media-centre/news-releases-campaigns/britain-launches-largest-trial-of-electronic-voting-in-europe
[xiii] https://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218Keyfindingsandrecommendationssummarypaper_27191-20111__E__N__S__W__.pdf
[xiv] https://www.nap.edu/catalog/11449/asking-the-right-questions-about-electronic-voting
[xv] https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2016/02/electoral_law_interim_report.pdf
[xvi] Speaker's Commission on Digital Democracy http:/www.digitaldemocracy.parliament.uk/
[xvii] Recommendation 26. Because of the decision to hold an election in 2017, the next UK parliamentary election is now scheduled for 2022.
[xviii] https://consult.gov.scot/elections/electoral-reform/
[xix] https://webrootsdemocracy.org/2018/01/28/welsh-government-announce-plans-online-voting-elections/
[xx] The main source for this section is the Speaker's Commission on Digital Democracy referenced above
[xxi] https://jhalderm.com/pub/papers/ivoting-ccs14.pdf
[xxii] http://www.sciencedirect.com/science/article/pii/S026137941630453X
[xxiii] http://www.democraticaudit.com/2013/10/03/the-estonian-experience-shows-that-while-online-voting-is-faster-and-cheaper-it-hasnt-increased-turn-out/
[xxiv] D. Bochsler, Can Internet Voting increase Political Participation? Internet and Voting 2010.
[xxv] P. Spada et al., Effects of the Internet on Paricipaption, World Bank Group February 2015
[xxvi] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/99553/Implementation-of-e-voting-in-the-UK-technical-issues.pdf
[xxvii] https://www.gov.uk/government/collections/individual-electoral-registration
[xxviii] http://www.electoralcommission.org.uk/find-information-by-subject/electoral-fraud/electoral-fraud-vulnerabilities-review?a=155335
[xxix] http://www.electoralcommission.org.uk/find-information-by-subject/electoral-fraud/electoral-fraud-vulnerabilities-review?a=164609

[xxx] http://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/194719/Proof-of-identity-scheme-updated-March-2016.pdf
[xxxi] http://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/194719/Proof-of-identity-scheme-updated-March-2016.pdf
[xxxii] https://www.lightbluetouchpaper.org/2007/08/02/electoral-commission-releases-e-voting-and-e-counting-reports/
[xxxiii] http://uk.businessinsider.com/twitter-found-more-russian-bots-trump-interacted-with-many-2018-1
[xxxiv] https://www.reuters.com/article/us-britain-eu-russia/russian-twitter-accounts-promoted-brexit-ahead-of-eu-referendum-times-newspaper-idUSKBN1DF0ZR
[xxxv] https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin
[xxxvi] this is a consideration in Scottish Single Transferrable Vote elections where the order of candidates' names has been shown to affect the number of votes each receives