WebRoots **Democracy**

the **cratos** principles

an essential guide to assessing online voting systems for use in elections

webrootsdemocracy.org

supported by:

phf Paul Hamlyn Foundation

Chowdhury, A. (2020) *The Cratos Principles: An essential guide to assessing online voting systems for use in elections.* WebRoots Democracy.

WebRoots Democracy is a London-based think tank focused on the intersection of technology and democratic participation.

webrootsdemocracy.org

contents

foreword

Online voting has the potential to truly transform democracies across the world. In theory, the reform can make elections more accessible, more accurate, and more affordable. Individuals living with disabilities and vision impairments can be empowered to cast their votes independently and in secret. Citizens and military personnel overseas can be confident that their voices will be heard. Current and future generations can vote in a way that aligns with how they live the rest of their lives: online. For any serious democracy, these should be viewed as vital objectives.

This ability to exercise democracy using a device in the palm of our hands is an ambition on the cusp of realisation. However, legitimate concerns regarding security and confidence in an online system cast shadows over the concept. In addition, given the black-box nature of the internet, it has often been a complex idea for decision-makers to grapple with and for the public to get behind.

In practice, online voting will inevitably take a different form to how traditional pencil and paper voting has worked. *Trust* alone may be not be enough and instead we may need to explore ideas like *verification*. Novel challenges may open the door to concepts such as *repeat voting* and necessitate *pseudonymous* voter identities. Equally, the opportunities enabled by the reform should encourage us to consider new thinking around accessibility, voter experience, and election information.

The Cratos Project (an abbreviation for **C**ertification and **Rat**ings for **O**nline Voting **S**ystems, and a play on a Greek root word of 'democracy') was established in order to define a set of principles from which to design and assess online voting platforms. The project was supported by the Paul Hamlyn Foundation and has drawn upon years of WebRoots Democracy's institutional knowledge in addition to insights gained from a series of expert roundtables, forums, and interviews held in Birmingham, Edinburgh, and London.

democracy = demos (common people) + **cratos** (rule, strength)

The result of the project are the *Cratos Principles* outlined in this report. In total, there are 33 which cover key aspects of accessibility, security, and user experience. Many of these principles, particularly those related to security, have historically split opinion amongst those in industry and academia and will, no doubt, continue to do so. However, the *Cratos Principles* are intended to provide clarity to those seeking it. Our proposed rating system does not require every principle to be met but, instead, weights heavier those principles which we deem to be most important.

The intended audience of this report are primarily civil servants working on online voting projects for the first time, students researching the subject as part of their educational programmes, and other interested individuals who are seeking an informed and detailed insight into this idea. The report is written with a UK context in mind, however much of the learning could and should apply to both public and private elections across the world.

Our hope is that this report serves as a useful tool for you as you embark on the implementation of pilots, the design of an online voting system, the creation of an audit process, or as part of wider research which you are undertaking on the subject. We hope you find the report insightful and thank you for taking the time to read it.

Areeq Chowdhury
Report author and
founder of WebRoots Democracy

the cratos principles

Our recommended principles for judging the suitability of online voting proposals for use in UK elections are listed below. There are 33 in total, covering *accessibility*, *security*, and *user experience*. They are not intended to be exhaustive but outline the essential requirements which determine strong platforms and frame the key criteria from which to distinguish proposals against each other.

Justifications and explanations of each of these principles are set out in the chapter *the Cratos Principles explained*. The principles are not presented in any particular order of importance or priority.

Accessibility

Online voting proposals should be rated higher for accessibility if they include:

1. Textual equivalents to visual information
2. Compatibility with text-to-speech software
3. Enlargeable text and images
4. Clear and accessible links
5. Inclusive colour schemes
6. Capability to be navigable by keyboard
7. Capability to be navigable by a single switch device
8. Closed captioning on video content
9. Sign language translations on video content
10. An easy read version of the platform
11. A helpline for those requiring assistance
12. Demonstrable input from users with disabilities in the design and development of the platform
13. Capability to switch to accessible versions, if necessary, without leaving the main voting application or website
14. Provision of information in alternative languages

Security

Online voting proposals should be rated higher for security if they include:

15. Capability for a voter to cast an independent, pseudonymous ballot
16. Capability for a voter to verify that their vote was recorded accurately
17. A pseudonymised public ledger of all votes cast
18. Capability to verify the identity of the voter prior to casting a ballot
19. A mechanism for repeat voting
20. Contingency plans in case of vote tampering both on an individual and large-scale basis
21. A mechanism of live-monitoring to detect malicious interference with the system
22. A mechanism for independently auditing every process, interaction, and instruction
23. Encryption and subsequent deletion of voter records and personal data
24. Contingency plans for interruptions in the availability of the platform
25. Guidance to inform voters about how to securely cast a ballot
26. Capability for a vote to be overridden by a vote cast in person
27. A commitment to share the platform's source code with relevant electoral administration staff and independent auditors

User experience

Online voting proposals should be rated higher for user experience if they include:

28. As few as clicks as necessary for a voter to cast a ballot
29. Capability to include images and information on individual candidates
30. Capability to include key information about the election
31. Social media integration
32. Randomisation of candidate positions on the ballot
33. Capability to cast and verify a vote on the same device and application/website

existing literature

Contemporary debate about remote online voting is often built upon assumptions agreed to by no-one. There is no international consensus on how a free and fair democratic process should be run. Different nations have come to different conclusions on what the voting age should be, how winners are decided, and what the separation of powers should look like. Similarly, there is a variety of thought into what the ideal make-up of a remote online voting platform should be. This is clearly reflected in existing literature on the topic. For example, the principle of voter identification is taken for granted in some countries but is absent in others. Some authors argue strongly in favour of an open-source process in the interests of security, and others argue the opposite but for the same reason.

Various papers and internet standards have been explored for the purpose of this report such as the *Common criteria for information technology security evaluation*[1], the *Council of Europe recommendation on standards for e-voting*[2], and the *W3C Web Accessibility Principles*[3]. Together, along with other studies, they provide a thorough overview of the ongoing debates and best practices around secure, accessible, and user-friendly platforms. In addition, various rating methods from a wide cross-section of society, such as healthcare and food standards, have been looked at.

Accessibility

Disability access to an independent, secret ballot is one of the key potential benefits of introducing a remote online voting platform. There is plenty of existing literature on how best to enable accessible websites. *The Cratos Principles* will aim to outline the criteria that should be met by online voting platforms and which groups should be enfranchised by the technology. Both *Web Accessibility*[4] and the *W3C Web Accessibility Principles* are good places to begin.

Key disability groups identified by *Web Accessibility: Improve the Web for Everyone* are as follows:

- Blind users
- Low vision and colour-blind users
- Users with motor disabilities
- Hearing impaired and deaf users
- Users with epilepsy
- Users with cognitive and intellectual disabilities

Best practice for developers designing accessible websites for each of these groups are also set out. These include solutions such as the use of HTML code to enable a textual equivalent to visual information to aid users with vision impairments, or the use of closed captioning or sign language to assist users with hearing impairments. These types of solutions will be essential in ensuring that an online voting platform provides an accessible alternative to existing methods.

The W3C (the Worldwide Web Consortium) is an international community where member organisations, staff, and the public work together to develop web standards. On their website, they provide great detail on standards for accessible online platforms. Similar to *Web Accessibility*, the W3C details a number of examples of web inaccessibility. They state that 'many sites and tools are developed with accessibility barriers that make it difficult or impossible for some people to use them.' This is a theme that equally arises in WebRoots Democracy 2017 report, *Inclusive Voting*.[5] Examples of the solutions proposed by the W3C include alternative text for images, keyboard functionality over mouse control, and transcripts for audio. They explain that some users with limited fine motor control cannot use a mouse, and that an accessible website makes all functionality available from a keyboard.

The W3C state that web accessibility relies on several components working together. This includes web content, user agents, and authoring tools. Web content refers to any part of a website,

[1] Common Criteria for Information Technology Security Evaluation, Common Criteria, 2019.
[2] Recommendation of the Committee of Ministers to member States on standards for e-voting, Council of Europe, June 2017.
[3] Accessibility Principles, W3C Web Accessibility Initiative, 2019.
[4] Web Accessibility: Improve the web for everyone (available in internet archives), 2016.
[5] Inclusive Voting, WebRoots Democracy, June 2017.

including text, images, forms, and multimedia, as well as any mark-up code, scripts, and applications. User agents refer to the software people use to access web content, including desktop graphical browsers, voice browsers, mobile phone browsers, multimedia players, plug-ins, and some assistive technologies. The authoring tools are software or services that developers use to produce web content, including code editors, document conversion tools, content management systems, blogs, database scripts, and other tools. These components will be equally important in the development of an accessible, online voting platform.

In 2018, the UK's Government Digital Service (GDS) published its own guidelines for how to make public sector websites and apps accessible.[6] In explaining the importance for accessible websites, they highlight that "the people who need them most are often the people who find them hardest to use." This problem was identified in *Inclusive Voting* particularly with regards to the increasing number of voter advice applications which provide information to voters on party policies. For some, these apps were inaccessible for users with disabilities. Common issues, according to the GDS, include websites being unnavigable using a keyboard, inaccessible pdf forms which cannot be read on screen readers, and poor colour contrast that makes text difficult to read for partially sighted users.

New regulations which came into force in September 2018 require the websites and mobile apps of public sector bodies to be 'perceivable, operable, understandable, and robust'.[7] Other requirements include the need for the publication of 'accessibility statements' which must contain details of content which does not meet accessibility standards, and for the provision, in reasonable time, of an accessible alternative. It may be the case that same requirements will be expected of an online voting system. Websites and apps will meet accessibility requirements if they comply with the international Web Content Accessibility Guidelines (WCAG) 2.1 AA accessibility standard.[8]

Security

The Common Criteria (CC) provides the ability to make comparisons between the results of independent security evaluations of information technology products in hardware, firmware, or software. It acts as a guide for the development, evaluation, and procurement of IT products with security functionality. The CC addresses the protection of assets from unauthorised disclosure, modification, or loss of use. These would all be key concerns for a remote online voting platform and are commonly referred to as 'confidentiality', 'integrity', and 'availability'. It is applicable to risks arising from human actions and non-human actions.

The CC, however, does not detail evaluation criteria for administrative security measures such as organisational, personnel, physical, and procedural controls. In a traditional election, this means it would be useful in assessing the strength and security of the physical ballot box, or postal vote, but not necessarily the additional organisational protections around it. Criteria for the assessment of the inherent qualities of cryptographic algorithms is also not covered in the CC.

Security in the CC concerns the protection of assets. These are entities that someone places value upon. In the case of elections, examples of assets would be the votes or perhaps the voters themselves. Given that value is subjective, lots of things can be classed as an asset. There would need to be a consensus on what the assets are in a UK election. Examples in the CC include:

- Contents of a file or a server
- The authenticity of votes cast in an election
- The availability of an electronic commerce process
- The ability to use an expensive printer
- Access to a classified facility

[6] Making your service accessible, Government Digital Service, 2018.
[7] The Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations, UK Government, 2018.
[8] Web Content Accessibility Guidelines 2.1, W3C, June 2018.

Assets are often in the form of information which is stored, processed, and transmitted by IT products. As would likely be the case in an online election, information owners may require that availability, dissemination, and modification of such information to be strictly controlled with assets protected from threats by countermeasures.

The CC states that the safeguarding of interest is the responsibility of owners who place value on those assets. It will, therefore, be important to consider countermeasures which can be taken by both the election administrators and the individual voters. Threat agents will also place value on the assets and attempt to abuse them contrary to the interests of the owner. Examples listed by the CC include hackers, malicious users, non-malicious users (who make errors), computer processes, and accidents.

To combat these threats, countermeasures are put in place consisting of both IT countermeasures and non-IT countermeasures. The CC states that asset owners should be able to defend the decision to accept the risks of exposing assets to threats. Two important elements to consider are whether:

a. The countermeasures are *sufficient* - if the countermeasures do what they claim to do and the threats to the assets are countered.
b. The countermeasures are *correct* – if the countermeasures do what they claim to do.

The CC recognises that asset owners (in this case, voters and election administrators) may lack the relevant knowledge, expertise, or resources necessary to judge sufficiency and correctness of the countermeasures. It also recognises that asset owners may not wish to rely solely on the assertions of developers due to bias. Asset owners may therefore choose to increase their confidence by commissioning an evaluation of these countermeasures. This is a significant debate within the digital reform of elections. Should election officials and members of the public be able to assess themselves whether an election is being run correctly, or should we look towards independent audits?

The sufficiency of countermeasures is analysed through a construct called the Security Target. The Security Target outlines the assets and threats and then describes the countermeasures in the form of Security Objectives. The countermeasures are divided into two groups which focus on the security objectives of a) the product and b) the operational environment. The CC does not assess non-IT countermeasures in the operational environment. The CC also assumes 100% correctness of the operational environment, however if it is incorrectly designed and implemented, the environment may contain errors that lead to vulnerabilities. This risk also arises in the correctness of the target of evaluation.

The CC and the approaches described within it will be essential for the design and implementation of a remote online voting platform. It makes clear that the countermeasures necessary for an online election will extend beyond the technology, itself, into physical property protections and informed use by individual voters.

The 2016 paper, *An independent assessment of the procedural components of the Estonian internet voting system* by Nurse et. Al provides further discussion on some of the operational challenges faced by online voting systems.[9]

More specific technical requirements are explored in the 2014 paper, *Design, development and use of secure electronic voting systems.*[10] The authors define technical requirements using the interdisciplinary method KORA and propose metrics to estimate the fulfilment of these requirements within online voting systems. For their target of evaluation, they consider three layers in their framework: human, computer (including hardware and software), and the network. It compares existing online voting systems to analogue election principles as we do within this report.

[9] An independent assessment of the procedural components of the Estonian internet voting system, Nurse, Agrafiotis, Erola, et al., University of Oxford, September 2016.

[10] Design, development and use of secure electronic voting systems, Zissis and Lekkas, March 2014.

KORA (Konkretiserung Rechtlicher Anforderungen / Concretisation of Legal Requirements) is a four-tier method for acquiring technical proposals based on legal provisions. These tiers are as follows:

1. Legal requirements are identified from the relevant parts of the constitution, relevant constitutional court decisions, and the opportunities and risks of the technology under investigation.
2. The legal requirements are made more concrete to so-called legal criteria by considering simple law regulations and decisions from other courts.
3. Functional requirements are deduced plus system integrity or the security layer.
4. A technical design proposal is deduced from the design goals and due to the systematic deduction, this proposal is supposed to be constitutionally compliant.

Building upon the research of others in this field, particularly around German electronic voting machines, they derived the following 16 requirements for an online voting system:

- System usability: The voting system is usable to all eligible voters.
- Accessibility: The voting system is accessible to all eligible voters.
- Vote integrity: The voting system ensures that each vote is correctly included in the election result.
- System availability: The voting system ensures that only eligible voters' votes are included in the election result.
- Uniqueness: The voting system does not accept more than one vote per eligible voter.
- System neutrality: The voting system does not influence the eligible voter's intention.
- Fairness: The voting system does not provide evidence about any eligible voter's intention before the end of the election.
- Secrecy: The voting system does not provide more evidence about an eligible voter's intention than the election result does.
- Anonymity: The voting system does not reveal who participated in the election.
- Individual verifiability: The voting system offers each eligible voter the possibility to verify that their intention has been correctly included in the election result.
- Archiving: The voting system stores relevant data after the election.
- Universal verifiability: The voting system offers any observer the possibility to verify that all technical requirements are enforced.
- Accountability: The voting system allows identifying the misbehaving party/parties in case of disputes resulting from the verifiability procedure.
- Understandability: The voting system is understandable to all voters.

These are criteria that will be explored for the *Cratos Principles* in order to see whether they are applicable within a UK context. Some of these requirements will not necessarily apply for UK elections, and others may be dependent on subjectivity e.g. understandability - are all voters required to understand all elements of an election process? The paper, however, sets a strong example of how the *Cratos Principles* can be approached and how a framework could be designed.

The authors state that in order to estimate to what extent online voting systems satisfy these requirements, it is necessary to specify how these technical requirements can be measured. For the functional requirements, most of the 16 requirements require individual metrics, whilst for the security layer, the same approach for all 16 requirements can be applied.

The paper proposes the use of the ISO[11] criteria (International Organisation for Standardisation) as metrics to estimate the effectiveness, efficiency, and satisfaction of the voting system. Metrics for effectiveness are measured in terms of Boolean variables that indicate if voters succeed in voting, and efficiency in terms of the time required to cast their vote. Satisfaction is

[11] About ISO, International Organisation for Standardisation, 2019.

measured in terms of Sauro's score for system usability. It recommends that accessibility is measured in terms of criteria derived within the Voting System Performance Standards Summary[12] and the US Election Assistance Commission's Voluntary Voting System Guidelines[13], which cover measures to enable voters with special capabilities.

In addition, the authors set out a list of potential adversarial capabilities as proposed by Neumann, Budurishi, and Volkamer in a 2014 paper[14] which are categorised into communication-based, corruption-based, computational, and timing related capabilities. These are set out below.

- Communication-based capabilities
  - The adversary can drop messages from the network channel
  - The adversary can read messages on the network channel
  - The adversary can inject messages on the network channel
  - The adversary can recognise the sender of messages on the network channel
  - The adversary can notice the usage of a network channel

- Corruption-based capabilities
  - The adversary can corrupt a human entity
  - The adversary can obtain objects from a voter
  - The adversary can send objects to a voter
  - The adversary can corrupt a computer system

- Computational capabilities
  - The adversary is computationally un-restricted

- Timing capabilities
  - The adversary has all of the above capabilities during a specified period of time.

Another paper from 2011, *Methodologies and technologies for designing secure electronic voting information systems*[15], sheds particular focus on the need for certification to provide trust and transparency over the system. Whilst a number of papers focus on potential technological challenges or solutions, few focus on the need and measures for public confidence. It is an area the Cratos project has covered throughout. The paper's author argues that the certification procedure requires focus on several important issues:

- Which authority is responsible for the certification process?
- Which criteria should be selected upon to accurately define an electronic voting systems requirements?
- Which components need to be checked to cover electronic voting efficiently?
- Which agent will conduct the technical analysis? Should the analysis be performed by public or private bodies?
- What shall be the availability of the certification procedure documents? (Public or private?)

Openness, the author argues, should not be limited only to source code, but to design methods, audits, and certification results. This is a key area of contention amongst online voting circles - whether the system and process should be open or closed. He states that there are at least three levels of openness, each with their own benefits, drawbacks, and peripheral issues:

1. Public disclosure of algorithms and protocols
2. Public disclosure of source code
3. Public or open contribution of source.

The author argues that security through obscurity (keeping parts secret) provides a false sense of

[12] Voting System Performance Standards Summary, State of California, 2019.
[13] Voluntary Voting System Guidelines, US Election Assistance Commission, 2019.
[14] Analysis of security and cryptographic approaches to provide secret and verifiable electronic voting, Neumann, Budurushi, and Volkamer, 2014.
[15] Methodologies and technologies for designing secure electronic voting information systems, Zissis, 2011.

security, limited verification, and vulnerabilities known by the wrong people.

An encryption algorithm, he states, is only believed to be secure when:

1. It is based on sound mathematics.
2. It has been analysed by competent, critical, and outside experts, and found to be sound.
3. It has stood the test of time.

As a new algorithm gains popularity, people continue to review its foundations. He argues that although a long period of successful use and analysis is not a guarantee of a good algorithm, the flaws in many algorithms are discovered relatively soon after their release. He states that the benefits of an open source design process for online voting systems are:

- A more secure system due to mass parallel testing, debugging, and monitoring
- Less complexity and higher quality
- Transparency
- Greater usability
- Greater accountability as design and test teams can be held accountable for not performing duties
- Independent analysis of voting software
- Interoperability

The split in opinion on open vs closed-source is apparent in WebRoots Democracy's *Secure Voting* report from 2016 in which there was division between the contributors on the question.[16] The debate centres around whether open-sourcing the code would provide any would-be hacker will full knowledge of how the software works, which may enable them to construct malware specific to that voting system.

In June 2017, the Council of Europe adopted recommendations on standards for e-voting. These are high-level standards but are useful in informing the design of the *Cratos Principles*. The key requirements highlighted by the Council of Europe are:

- Universal suffrage (accessible and optional method of voting)
- Equal suffrage (unique identification, one person, one vote)
- Free suffrage (voter under no undue influence)
- Secret suffrage (secrecy of the ballot)
- Regulatory and organisational requirements (legislative changes)
- Transparency and observation (transparency in all aspects)
- Accountability (auditability)
- Reliability and security of the system (security and authorisation)

Significantly, these standards do not mention voter verification of results, and voter identification is not yet a requirement for UK elections. Additionally, how secret should ballots be? The secret ballot in a UK context does not currently mean total anonymity as ballot papers can be traced back to the individual voter under particular circumstances (e.g. when the result is contested).

User experience

Various guidelines exist for how best to optimise the user experience of websites and mobile apps. Google's 2015 'Think with Google' piece *Mobile Optimization to Improve the User Experience* speaks of the need for 'immediate gratification'.[17] With the various security requirements that may need to be put in place for an online voting system, the balance between security and user experience is delicate. Can an online alternative meet its potential for being an easier, stress-free method of voting if it is lumbered with multiple security checks that delay the immediate gratification of casting the ballot? This is a key question, often overlooked in existing literature, which will need to be answered and measured if online voting is to be the method of choice in future elections.

Google's research looks at the reasons why people switch from one app or website to another and what elements of user experience deter them from venturing further. It also highlights the following three key methods to optimise mobile user experience:

[16] Secure Voting, WebRoots Democracy, January 2016.

[17] Speed is key: Optimise your mobile experience, Think with Google, September 2015.

1. Eliminate steps - the more steps involved in a mobile experience, the more likely a user is to make an error.
2. Anticipate needs - the app should understand what a user wants before they want it.
3. Minimise loading time - research shows that 40% of shoppers will wait no more than three seconds before abandoning a retail or travel site.

Olembo and Volkamer's chapter *E-voting system usability: Lessons for interface design, user studies, and usability criteria* of the 2013 publication *Human-Centered System Design for Electronic Governance* explores conference proceedings, journal articles, and other secondary sources focusing on the usability of e-voting systems.[18] In particular, the chapter focuses on remote e-voting systems which provide cryptographic verifiability. The authors highlight four key reasons for the importance of user experience in online voting platforms:

1. Anyone who meets the voting age requirement should be able to use an online voting system to cast their vote, including first time voters, the elderly, and those who do not frequently interact with technology.
2. A voter should be able to easily express their wishes and the interface design should not cause mistakes nor influence the voter's decision.
3. Since elections are held infrequently, voters are likely to be novices with these systems.
4. Poor user interfaces are likely to create frustration which may reduce acceptance amongst voters and decrease voter turnout.

The authors look at various areas of interest such as verifiability, the US' Voluntary Voting Systems Guidelines (VVSG), the ISO 9241-11 Standard[19], and human computer interaction (HCI) usability evaluation techniques. They also make a number of specific recommendations for how to design the interface and where information should be placed. This is not within the scope of the Cratos project but has been explored in order to inform the principles and ratings framework.

Bederson's 2003 paper, *Electronic voting system usability issues*, looks at problems surrounding user experience on e-voting machines and highlights concerns around accessibility, technical experience, bias, and verifiability.[20] This article is particularly useful in identifying the potential impact on elections of procedural reforms. For example, the positioning of a candidate on a ballot paper can be a contentious issue as some believe it may impact the number of votes a candidate receives. Do the same issues arise with e-voting? Whilst a relatively old paper, with regards to research about technology, it raises a number of important questions which are still relevant to both in-person and remote electronic voting systems.

The existing literature on this topic is lacking with regards to a method of measuring and weighting different factors that make up an optimal user interface for online voting platforms. This is something we have focused upon throughout this project in our interviews, roundtables, and other forms of research.

Rating methods

There is a wide variety of methods which could be used to rate online voting platforms. The key aim of the Cratos Project is for this ratings system to be relatively straightforward and for it to be used by a range of stakeholders such as civil servants, election administrators, and politicians. The ratings are not intended to be used as an accreditation mechanism but as a tool of informing key users on the suitability of various online voting platforms. Various rating methods such as the engineering design process, 5 star and thumbs up, and the scoring system used by the National Food Hygiene Ratings have been explored, in addition to existing rating methods for websites.

[18] E-voting system usability: Lessons for interface design, user studies, and usability criteria, Olembo and Volkamer, January 2013.

[19] Ergonomics of human-system interaction – Part 11: Usability definitions and concepts, International Organisation for Standardisation, 2018.

[20] Electronic voting system usability issues, Bederson et al, April 2003.

Tips for effective rating scales as set out by Qualtrics, the evaluation and experience management company, aim to minimise the amount of subjectivity involved.[21] The five basic goals for a ratings method are as follows:

1. It should be easy to interpret the meaning of each scale point.
2. The meaning of scale points should be interpreted identically by all respondents.
3. The scale should give enough points to differentiate respondents from one another as much as validly possible.
4. Responses to the survey rating scale should be reliable, meaning that if the same question is given again, each respondent should provide the same answer.
5. The scale's points should map as closely as possible to the underlying construct of the scale.

In engineering, ratings form a key part of the design process, as set out in Khandani's 2005 paper.[22] It is used to trial different design options or solutions to problems. The first step is to decide what the rating criteria should be and to give each criterion a weighting. Examples in engineering might be 'safety' or 'durability'. For online voting platforms, the criteria will be the *Cratos Principles*. Each solution (or platform) is then assessed against the criteria and given a mark (e.g. out of 10). In most cases, in engineering, this decision is subjective. The mark is then multiplied by the weight of the rating factor, and scores are then compared for each solution. This has been chosen as the preferred and most suitable method for the Cratos Project.

The Food Hygiene Ratings follows a similar system to the engineering design process, with scoring done against three key criteria.[23] The scores are given out of 30 for each criterion and then added together to create a total score. This then indicates where an establishment ranks on the five-tier rating.

The five star and thumbs up method is a very simple but entirely subjective method of rating and would thus be inappropriate as a means of measuring each principle. However, the five-star method in particular, could be used as an option to visually present the ratings of online voting platforms. However, due to the significance of online voting platforms, using a four-star rating for example could be misleading as to how reliable said platform is. A better and clearer option to present the ratings would be through alphabetical ratings, e.g. AAA, AAB, ABB etc.

Discussion

As the main concern, across the board, with online voting is security, it is understandable why the vast majority of literature focuses on this aspect of the reform. Inevitably, it is a core, and potentially contentious, part of the *Cratos Principles*. However, there has been lots of research undertaken on our other two areas of interest: accessibility and user experience. The work on accessibility, in particular, is very strong. Measuring user experience may be more difficult as it may involve an element of subjectivity and will intersect heavily with the accessibility and security principles.

The key challenge here will be to bring together all of these different strands and form a comprehensive, yet easy to understand, method of measuring these factors on their own, but also together. What will a weak user interface but strong security mean for an online voting system? Would voters take to it if the process is cumbersome? What does a user-friendly platform look like for voters from different walks of life? These questions have been kept at the forefront throughout this research.

The *Cratos Principles* aims to add to the existing literature on the subject, focused particularly on the United Kingdom. The addition of an understandable method of rating platforms alongside detailed principles for an optimal system should move existing conversations forward away from theory and hypotheses to practical, real-world applications of the technology.

[21] Three tips for effectively designing rating scales, Qualtrics, June 2018.
[22] Engineering design process, Khandani, August 2005.
[23] Food Hygiene Rating Scheme, Food Standards Agency, 2019.

existing principles for paper ballots in the uk

When approaching the question of online voting it is important to contextualise it within the existing system of paper-based voting and not to look at it within a vacuum. Do online voting platforms need to meet the criteria of polling station voting or postal voting? Can it be sufficient even without meeting the criteria or must it go even further? These are the questions that need to be answered when approaching the reform and when assessing potential platforms.

Putting aside the registration process for voting, a brief outline of how existing methods of paper-based voting work and the principles which are being achieved is explained below.

Sealing of the ballot box

Prior to the opening of the poll, the Presiding Officer seals the ballot box at the polling station after having shown all those entitled to be present that the box is empty. There are various designs of ballot boxes in use within the UK, however regardless of the design, they are to be properly secured. This provides assurance that the ballot boxes haven't been pre-filled by malicious actors.

Voter identification

There is currently no explicit method of voter identification with either in-person voting or postal voting, although the UK Government is committed to introducing it as a requirement in future. There is, however, implicit identification through voters needing to confirm their name and address. On entering the polling station, staff inside ask for a voter's name and address and check they are on the electoral register. They then hand the ballot paper to the voter and make a note of the ballot paper number.

What is being achieved here is that the polling station staff member is given reasonable assurance that a given individual is eligible to vote in the election as they match both a name and address on the electoral register. They are also able to mark that the voter has cast a vote and prevent any other individuals who arrive later from attempting to impersonate the voter.

With postal voting, voters complete and sign the postal voting statement which is placed together but separately from the envelope containing the postal vote itself in a larger supplied envelope.

Casting an independent, secret ballot

On receiving the ballot paper, the voter takes it to a booth and marks their decision using a pencil provided. The booth is not entirely private in order to allow poll workers to observe whether or not another individual is pressuring the voter. The voter then folds their ballot and places it into the ballot box.

The objectives achieved here is that a voter is able to cast a vote in secret and without fear of a malicious actor pressuring them to vote in a certain way. In addition, polling station staff are given reassurance that the vote cast was done without peer pressure. The voter leaves the polling station with confidence that their vote has been marked in the way they intended and placed into the ballot box. With proxy voting, an individual appointed by the voter undertakes this process on their behalf.

For voters with vision impairments and disabilities, they can request assistance from the staff at the polling station and are even able to mark the ballot on the voter's behalf. Whilst, in theory, this enables greater accessibility for the voter, in practice it can lead to voter secrecy being sacrificed.

Transportation of ballot papers to the count centre

The Counting Officer is responsible for the transportation of ballot boxes and other election materials to the count centre. Electoral Commission guidelines indicate that a lone Presiding Officer would be able to transport the ballot box to the count centre, however if there is "too much to carry" a poll clerk may be asked to assist. The ballot box is not to be left unattended at any time. The principle being achieved here is that the ballots are delivered by a trusted and accountable individual.

Counting the votes

To further demonstrate the integrity of the vote, the ballot boxes are publicly and ceremoniously

emptied onto tables at the count centre with the empty boxes shown to the observers. The ballot papers are then counted and checked against the expected number of ballot papers. If the numbers do not match, there are recounts until they do match or the same number of ballots is recorded twice in succession.

Before counting the votes, the ballot papers from different boxes are mixed and then allocated to count teams who sort the papers by the candidate(s) voted for. Once the sorting is completed, the total number of votes plus the total number of rejected votes are compared against the total number of ballot papers. The provisional results are then shared with candidates and their agents who may request a recount with there being no limit on how close a result has to be to qualify for a recount and no limit on the number of recounts that can be requested. Principles of secrecy, accuracy, and candidate confidence are being achieved by these measures.

Overview of the principles achieved in paper-based voting

Principle	In-person	Postal	Proxy	How is it achieved?
Assurance that the ballot box has not been tampered with prior to the election.	✓	✓	✓	Public sealing of the ballot box.
Assurance that the ballot box has not been pre-filled with votes.	✓	✓	✓	Public sealing of the ballot box.
Assurance that the voter is who they say they are.	✓	x	✓	Matching a name and address with the electoral register.
Assurance that the voter is eligible to participate.	✓	x	✓	Matching a name and address with the electoral register.
Casting a secret ballot.	✓	x	x	Voting alone in a booth at the polling station.
Assurance that the voter is not being peer pressured to vote a certain way.	✓	x	x	Observation by poll staff that the voter is voting alone.
Assurance that the vote cast is as intended.	✓	✓	x	The voter observing their vote go into the ballot box.
Assurance that ballots are not tampered with in transit to the count.	✓	✓	✓	Assigning a trusted official to transport the ballot boxes to the count centre.
Assurance that the ballots are not tampered with at the beginning of the count.	✓	✓	✓	Public emptying of the ballot boxes.
Accuracy over the number of ballots.	✓	✓	✓	Cross-checking the number of ballots with the expected numbers from polling stations.

Principle	In-person	Postal	Proxy	How is it achieved?
Assurance that the ballot boxes cannot be used to trace back individual voters.	✓	✓	✓	Mixing the ballots from different ballot boxes.
Assurance that all votes cast have been counted.	✓	x	✓	Cross-checking final count number with the total number of ballot papers.
Assurance over the accuracy of the final count.	✓	✓	✓	Recounts upon request.

accessibility of online voting platforms

For most citizens, the appeal of remote online voting is the convenience it offers: a digital ballot box in the palm of your hand. No longer must voters worry about turning up to a local church before the school run or after work. No longer do overseas voters have to navigate the complexities of a foreign postal service or pray that their ballot paper arrives back to the UK on time. Online voting can reduce the cost of participation and make it easier for everyone. For others, however, online voting represents so much more than that.

If someone has a severe disability, participation in the existing paper-based system may be impossible. Perhaps they have a bed-bound disability. Maybe they are vision-impaired. For these voters, online voting is more than an issue of convenience, it is a necessity. Given that any and all of us can obtain a disability throughout our lives, it would be a mistake to view this as a minority concern.

WebRoots Democracy has made this cause central to its calls for pilots of remote online voting, and the need for an accessible method of independent voting underpins the Cratos Project. This chapter outlines some of the key challenges and concerns related to this and provides background to the accessibility section of the *Cratos Principles*.

Vision-impairments

In the UK, there are currently five different methods of casting a ballot for voters with varying levels of impaired vision. Recognising the challenge faced by such voters, they are designed to enable them to cast a ballot *independently* and in *secret*. This ability to cast an independent, secret ballot is enshrined in human rights law and is the foundation of democracies across the world. However, the paper-based system of voting has been criticised for being insufficient in enabling this right.[24] Those who are unable to see at all or are unable to read braille can find it impossible to cast a vote independently and in secret.

This problem was described as a 'civil rights issue' in the USA when, in 2013, a federal judge ordered Maryland to allow blind and disabled voters to fill out absentee ballots online.[25] Similarly, in 2011, advocacy group Vision Australia argued that the Government 'has an obligation to enact the necessary legislation and provide sufficient resources to facilitate the development and continuation of equitable voting practices.'[26] One of the methods they said would enable their service-users 'to cast an independent, secret ballot' was the introduction of an online voting option 'in which votes are cast using an accessible website.' New South Wales, in Australia, has since introduced remote online voting in elections.

The current provisions, here in the UK, are as follows:

Large print ballot form

Voters with vision impairments can request a large print copy of the ballot paper to take into the polling booth with them, which they can then use as a reference. The voter then uses the large print copy to read all of the information on the ballot paper but must still cast their vote on standard size print ballot paper. This provision is not particularly helpful for voters who struggle with standard size print ballot papers or who are fully blind.

Tactile voting device

If the voter has difficulty completing the ballot paper, they are able to request a tactile voting device at the polling station to help them mark their vote in the correct place. This device has a sticky backing, which attaches at the top of the ballot paper. It has numbered lift-up flaps written in braille, directly over the boxes where you mark your vote.

The voter will need to use the large print ballot form or ask someone (a companion or polling

[24] Visually impaired denied right to vote in secret, Third Force News, May 2017.
[25] Court case: Voting via the Internet is a civil rights issue for disabled, Al Jazeera, July 2014.
[26] Access to Voting (Word Doc), Vision Australia, July 2011.

station staff) to read out the list of candidates to them. The voter then needs to remember the number of the candidate they wish to vote for, lift the flap with the same number, and mark an X in the box. Finally, the voter detaches the tactile device and folds their ballot paper in half before posting it in the ballot box.

This is the primary method for a voter who is fully blind to cast an independent and secret ballot. However, with the rise of technology has come the fall of braille. For this reason, and others (such as voters losing their sight later on in life) it is now estimated that just 1% of the vision impaired population in the UK can read braille. Tactile voting devices are, therefore, rendered useless to the 99%.

Help at the polling station

If the voter has difficulty with both the large print ballot form and the tactile voting device, they can request someone to help them at the polling station. That person can help guide the voter between the entrance, desk, polling booth, and ballot box. They can also cast the vote on their behalf. The person aiding the voter could be a companion or polling station staff. Any companion must be a member of the voter's immediate family over 18 years old, or a 'qualified elector' – which is someone who is legally able to vote in a UK election. In this method however, the voter sacrifices their right to independence instead placing their trust in another person.

Vote by proxy

Any voter who is unable to get to a polling station to vote can appoint someone they trust to go to the polling station to vote on their behalf. This is called voting by proxy. Unlike postal voting, a reason must be provided for a proxy vote. Voters can cite their vision impairment as a sufficient reason for a proxy vote.

The vision impaired voter needs to register to vote by proxy at least six working days before the election by completing an application form and sending it back to their local electoral registration office. Unless the voter is registered blind, they will need someone to support their application such as a GP or a social worker.

Postal voting

All voters can apply to vote by post rather than going to a polling station. If the voter has registered to vote by post, they will be sent the ballot paper in the post. A vision impaired voter can then cast their vote in their own home using their own magnifiers or equipment, rather than going to the polling station. The voter can also request assistance at home, including a tactile voting device, a large print ballot form for reference, and help with mailing their completed ballot form. This is possibly the best option in terms of providing independence and secrecy for the voter. It is dependent on the voter having specialist equipment required in order to read the ballot paper.

Motor disabilities

The mainstream method of voting and the existing provisions for remote voting ultimately privilege able-bodied voters. If a voter can physically get up and walk to the polling station or to the post box, then they are able to participate in elections. If, however, they have a motor disability which leaves them bedbound or unable to walk, voting becomes significantly more difficult. An independent and secret ballot is no longer an option. They must, instead, depend on the arrangement of a proxy vote, trusting another to cast their vote on their behalf.

These challenges are well-documented. For many voters with disabilities, physical access to polling stations can be difficult. This can be due to barriers such as steps at the entrance, heavy closed doors, and narrow corridors. The level of inaccessibility can be much worse when polling stations are located in obscure venues such as portable cabins, caravans, or in fields. In addition, in some cases, disabled people find that they cannot park near the polling station, can be disorientated by too bright/not bright enough lighting, and find that the voting booths themselves are too high or too low.

Can this be remedied with remote online voting? In 2010, the disability charity, Scope, called for the reform after 35% of participants they interviewed

for their *Polls Apart* study said they would prefer to vote online.[27] In the report, Scope said:

"For some groups of voters, both polling station and postal voting continued to be fundamentally inaccessible. Those with complex physical impairments still had to rely on others to physically mark their ballot paper on their behalf, denying them their right to a secret ballot. New technologies are now being used by disabled people to improve accessibility in every part of their lives, and the potential of it to revolutionise voting remains considerable."

Research by Leonard Cheshire Disability following the 2015 General Election found that 24% of disabled people found it difficult to vote in person at polling stations.[28] The problems their research highlighted include:

- No level access or disabled parking spaces available at some polling stations
- Inaccessible voting booths and ballot boxes
- Polling station staff lacking training to help

Enabling access to democracy for these voters is the biggest potential benefit of remote online voting. Current provisions are provably insufficient and, as a result, the right to an independent, secret ballot is sacrificed by necessity.

Learning disabilities

Voting has very particular challenges for those with cognitive disabilities and represents one of the most significant challenges with regards to accessibility in online voting.

Mencap, a charity which supports 1.4 million people with learning disabilities, provided information for WebRoots Democracy's 2017 *Inclusive Voting* report which showed that 17% of their surveyed members had been turned away from a polling station because they had a learning disability.[29] They highlighted that this is in contradiction to electoral law which states that voters cannot be turned away from polling stations on account of a 'lack of capacity' and that this can only be decided by a court.

A parent detailed their experience in Scope's *Polls Apart* report as follows:

"I took my son who has learning disabilities to vote. I was disgusted to hear one of three people at the polling station say 'that's another spoilt paper' and the other two agree. In future we will go for postal voting so that we don't have to put up with these sorts of comments."

Given the difficulties for voters with particularly severe cognitive disabilities, special consideration for this will need to be considered in the implementation of remote online voting. Failure to create an accessible platform would represent a failure to take advantage of the full potential of remote online voting.

Overseas voters

An often-cited concern before, during, and after elections are the difficulties faced by voters overseas. These may be citizens temporarily working or living abroad, or it may include members of the armed forces who are long-term postings in remote terrains. Akin to voters with severe disabilities, their options are postal or proxy voting. In the UK, the Government and Electoral Commission advises overseas military personnel to vote via proxy instead of post as 'there may not be enough time for your postal vote to reach you and be sent back before voting closes.'[30]

Challenges with voting whilst overseas include difficulties in navigating a foreign postal service, delays in international post, and lack of access to a reliable postal service. These challenges can occasionally lead to postal votes not arriving to the voter on time or not arriving to the count on time. According to a 2017 survey of armed forces personnel by the Army Families Federation, 91% said that they believe online voting should be an option for them.[31]

[27] Polls Apart, Scope, July 2010.
[28] Barriers to voting – one in four disabled voters found polling stations inaccessible, Leonard Cheshire Disability, May 2015.
[29] Inclusive Voting, WebRoots Democracy, June 2017.
[30] Military Voting, WebRoots Democracy, August 2017.
[31] Ibid.

English as a second language

Something which doesn't often arise in conversations on election accessibility is the problem of language discrimination. Barriers for non-English speakers arise in all aspects of the electoral process in voter registration, candidate information, and, of course, the casting of a vote. In 2018, Kasimir Rantzau (who speaks English as a second language) wrote a piece for the WebRoots Democracy website on the subject as part of the research for the Cratos Project.[32] Explaining the predicament, he wrote:

"Being a non-English speaker, I am not automatically excluded to vote. Hypothetically, I can ask my English-speaking cousin to translate my postal vote registration and the subsequent issuance of my vote. Through this help, I am able to issue my vote. If eligible, I can also choose to issue my vote through a proxy. I ensure a person I trust with my vote. In addition, through the nature of such proceedings, I am confined to the trust and support of a third person."

Similar to physical disabilities, language barriers can also prevent a voter from accessing their human right to cast an independent, secret ballot. In the UK, there have even been calls to ban the use of non-English or Welsh languages at polling stations due to fears around voter fraud. The implications of this could be significant disenfranchisement for thousands of voters across the country.

More than 800,000 people across the UK cannot speak English or speak it poorly. In particular, this problem is experienced by Polish, Panjabi, and Bengali speakers. In addition, this also affects almost 10,000 people who speak British Sign Language. It is feared that this problem may already be affecting voter registration levels with 19% of ethnic minority voters not being on the electoral register compared with 7% of White British voters.

In 2015, the BBC interviewed Liz Ball, a voter who is deafblind and communicates through tactile fingerspelling.[33] She described the existing system as 'antiquated' and said:

"It still doesn't take account of technology or the shift in societal attitudes to disability. It's about time that as a country we got our act together to make sure that everybody can vote without being disappointed or frustrated by that process."

She said that online voting 'would not just make it easier for people with blindness, but those with other disabilities would benefit, too'.

So, can online voting help remedy this problem? Whilst cost implications may render ballot paper translations impractical, the internet provides an opportunity to do so inexpensively. An online voting platform could be made more accessible with translations of voting instructions in British Sign Language or any other language as the local election authority sees fit.

The big benefit of introducing online voting is the removal of barriers to voting. For most voters, these barriers impede the convenience and ease of voting. For those with disabilities, these barriers impede human rights. The human right, as recognised in international and domestic law, for citizens to be able to cast an *independent* and *secret* ballot in elections is impossible to access in the existing paper-based system.[34] To enable this right with an online voting platform should be the number one priority for all involved in its development, promotion, and implementation.

[32] The local elections and language discrimination, Rantzau / WebRoots Democracy, April 2018.
[33] Why do disabled people feel ignored when it comes to voting? BBC, March 2015.
[34] Article 3 of the First Protocol: Right to free elections, Equality and Human Rights Commission, May 2017.

security of online voting platforms

The security of any voting method, whether paper-based or online, is critical to ensuring trust and confidence in the election outcome. Whilst not an exhaustive list, we have explored the key security challenges to implementing an online voting platform in elections. Building on our previous research in this area, we sought views from a wide spectrum of experts in the field from governments, academia, and the industry. These findings are outlined in this chapter and provide background to the *Cratos Principles*.

Protection of assets in an online election

With online voting there are a number of assets both offline and online which need to be protected. These include the following:

- Voter information (e.g. any personally identifiable information)
- Political preferences of the voter
- Election information (e.g. encryption keys, information on accessing the infrastructure, the results of the election)
- Integrity of the ballot
- Integrity of the result
- Logs (e.g. any event taking place during the election)
- Information about the ongoing election (e.g. how many ballots have been cast, who has voted, what existing attacks are ongoing)
- Devices used to vote in the election
- Public trust in the election
- Availability of the election system
- Knowledge about the election (e.g. how the processes are run, validation of the votes)
- People (e.g. staff involved in running the election)

Many of these are also assets in existing paper-based voting systems but may take a different form in an online election. What is clear, however, is that the current system can be highly decentralised across and within the 600+ constituencies in the UK. Replicating such qualities can help provide greater assurance over the robustness of online voting platforms.

Personally-identifiable information is available in the existing paper-based voting system in the UK, particularly with postal voting. In essence, what protects postal ballots from malicious actors matching the vote, and the political preferences of the vote, with the voter is an envelope. With in-person voting, the personally identifiable information can be found on the back of a ballot paper which contains a serial number which could, in theory, be traced back to the name of the voter. This mechanism is in place in order to assist with legal challenges to an election result and is the only method for a voter to be able to verify that their vote has not been tampered with.

A common theme throughout this paper is the idea of assurance vs guaranteed security. Assurance is the idea that we can have a level of trust in a process based on the number or types of protections that have been put in place. Guaranteed security is the notion that a system is infallible to attack. Whilst used as a yardstick for electronic voting systems by a number of commentators, the idea of guaranteed security does not really exist anywhere online or offline, only assurance is possible. So, with the main measures in place for protecting personally identifiable information and political preferences being decentralisation, physical barriers, and trust in individuals, we can only have assurance that this information is secure. The same should be true of online voting and sufficient assurances should be in place. Failure to do so risks the integrity of the ballot.

Critical information related to the infrastructure of the online voting system should undoubtedly contain security controls including everything from the encryption keys used, to the device and browser used by the voter. However, the design of the system should build in the assumption that the infrastructure will be compromised and that votes will be tampered with. Therefore, the most important assets are the integrity of the result and the public's trust in the outcome. A robust online voting system should focus on detection of illicit activity and especially the tampering of votes. A method to allow individuals to verify their votes once they have been cast and transparency over the count of the vote could be one solution to this challenge.

Maintaining the availability of the platform is another important challenge of online voting

albeit not a unique one. In the existing system, the asset of availability is dependent on the functioning of the postal service and the accessibility of polling stations. An example of where availability can be affected is the 2016 Brexit referendum during which flooding in parts of the South East of England resulted in some polling stations being forced to close in addition to severe disruption on public transport networks.[35] An attack which could affect the results of an election without having to alter individual votes, would be to shut down the online voting portal altogether through a distributed denial of service. This must be factored into the design of any online voting proposal and there needs to be contingencies in place. This may be difficult to achieve if the online election takes place on a single day or the same day as the in-person election.

Responsibility for the protection of these assets will fall upon the developers, the election authority, and the individual voter. With postal voting, measures are taken by the election authority, the printers, and the postal service to protect the integrity of the vote, however significant responsibility and trust is placed in the voter to take their own precautions. This may involve, for example, completing their ballot in private, taking care of the physical ballot paper, properly sealing the envelopes, and submitting the vote on time. The same approach should be taken with remote online voting. Developers and the election authorities should be able to demonstrate the measures they have taken to protect the vote and educate the voter, but the voter, too, has a responsibility in ensuring others do not tamper with their vote or login credentials.

Anonymity vs pseudonymity

A key issue in the commentary and literature which is often accepted without question is the concept of voter anonymity. Whilst in a number of countries around the world, the identity of the voter has to be entirely untraceable, this is not the case in the UK. The idea of a 'secret ballot' in the UK is related more to an individual being able to vote in private and for it to be highly inaccessible for anyone to know how they voted. During investigations of electoral fraud, and with strict conditions, it is possible to trace a ballot paper back to the individual voter. This is done using the serial numbers on the back of each ballot paper and matching it with the voter's name as recorded on the voter logs at polling stations. The UK, therefore, has a principle of voter pseudonymity (where the voter's identity is hidden but traceable through a serial number) rather than voter anonymity (where the voter is entirely unidentifiable).

The clear benefit of voter pseudonymity is that it provides a mechanism, and the only mechanism, for verifying that a vote was recorded as cast in a paper-based election. In instances of voter fraud investigations, it would be possible to show an individual their ballot paper and to have them confirm whether that was indeed their vote. Without such a process, it would be impossible for an individual to verify whether or not their vote was accurately recorded in the count. Whilst some argue that the entire process should be anonymous, the ability to detect fraud and interference, which the principle of pseudonymity provides, is a critical one. Regardless, of these arguments however, there is a question mark over whether anonymity would be achievable in any online voting system. For example, some have argued that even processes such as encryption and hashing should be defined as providing pseudonymity instead of anonymity.

The secrecy of the ballot, whether anonymous or pseudonymous, is a fundamental pillar of democracy and must be protected. As with many concerns that are raised in this conversation, the risks are not exclusive to online voting and appear in other forms of voting such as postal and proxy voting. In postal voting, protections around secrecy are not infallible from either peers or from those handling the votes. With proxy voting, trust is placed in friends, relatives, or carers. The difference with online voting is the fear surrounding the potential scale of the risk. With postal and proxy voting, the risk may exist, but it is easy to see how the likelihood and impact would be minimal. To ensure trust in the process, an online voting system must aim to replicate the model of postal and proxy voting, ensuring that the likelihood and impact with associated risks are kept to a minimum.

[35] EU referendum voters wade through water as floods hit south-east, Guardian, June 2016.

Open vs closed source

The question of whether or not the design and processes of online voting systems should be open-sourced is one which divides opinion both in the electronic voting industry and within academia.

The main arguments for open sourcing a platform are based on the belief that allowing the code to be reviewed by an unlimited and broad audience will strengthen the system and provide greater reassurance for voters that the software is robust enough for elections. The arguments against doing so are two-fold. Firstly, open sourcing the code not only provides access for beneficent hackers, but malicious ones, too. Full knowledge of how the software works lowers the barriers to attack and may enable a malicious hacker to construct malware specific to that voting system. Secondly, publishing the ins and outs of how a system works may act to disincentivise the commercial growth of the electronic voting sector. Developers may lose a competitive advantage by publishing how their system works if their rivals do not also do so. The incentive for spending money on creating an online voting platform may disappear if developers are forced to publish their source code online.

Given that trust and transparency is key to the success of online voting, there is an increasing movement towards open source online voting software. Some developers share the code for the entire voting system, including the voting, tallying, and auditing software on GitHub, a popular website for source code management and distributed version control.

The democratic ideals of open source also add weight to its potential requirement for online voting platforms. The current paper-based voting system is open source in the sense that the public are able to scrutinise the voting process if they wish. The best example of this in the UK is the election count itself, where observers can be appointed to watch over the ballot count. However, the entire voting process is not open-sourced. For example, the public does not have access to the production of paper, ballot boxes, or vehicles which transport ballot papers from one location to another. Instead, only the critical parts of the election process are made public.

However, whilst sharing the source code of election software makes it easier for independent, third parties to detect flaws in a system, it does not guarantee its security or that the published code will be the same as the one actually used in the election. It also limits awareness and understanding of the software to specialist, IT-literate individuals. This delegation of trust to specialists is something which will be necessary in any realistic implementation of online voting in elections.

The alternative, or compromise position, would be for developers to share their source code with a select, trusted group of individuals. These may be auditors, election administrators, or white-hat hackers. This allows for independent review of a platform whilst limiting access to full knowledge of a system to malicious individuals or states. This position, sometimes referred to as *disclosed source* is one which is adopted for the vast majority of a nation's critical infrastructure. A state would not dream of publishing the full details of how its weapon management systems operate due to the clear risks to national security. There is a strong argument that elections should be viewed through this prism of national security, too.

Archiving of votes

The challenges of a creating a secure online voting system doesn't end with the announcement of the election results – this is only half of the task. To ensure integrity in the vote, there must be a process in place to ensure that the results can be contested should there be any irregularities or valid reasons to suspect the outcome. With paper ballots, this is accommodated for, in part, by the storage of ballot papers for a fixed period of time after the election. Can the same be achieved, securely, with online voting?

In the UK, votes are stored for a year following an election before being incinerated and destroyed. The question for those seeking to implement an online voting option is whether the same can and should be replicated. Should online votes similarly be stored and destroyed, or are there alternative methods of verification?

As with all aspects of online voting, when comparing the method to existing paper-based elections, the focus should be on the purpose of

an action rather than the exact replication. The purpose of storing and incinerating votes is to achieve two things. The first is to ensure that any allegations of corrupt or illegal practices can be investigated by the authorities. The second is to protect the secrecy of the ballot. The answer to this is to enable voters to be able to verify their votes themselves. When compared to in-person voting or the other method of remote voting, postal voting, this adds an extra layer of security and trust for the voter.

Transparency over the count will also be key here. If voters can witness the vote count themselves and know that their vote is within that count, correctly recorded, this would alleviate concerns regarding corruption. However, full transparency of the count, published online, would mean that a permanent, indestructible record of the vote would exist. The most challenging aspect of this area therefore is to protect the secrecy of the ballot and ensure that votes cannot be traced back to voters by anyone other than the voter themselves.

Many of the contributors to the 2016 paper, *Secure Voting*, highlighted the need to separate, physically and digitally, the database used to issue voter information and the database used to store the votes cast.[36] Decentralisation of databases will be essential here. This challenge, whilst difficult, is not unique to voting. The same approach should already be in place for all sensitive data which governments hold whether it be information concerning national security, benefit claims, or medical records.

Safeguards from peer pressure and vote-buying

One of the most common questions which arise when the potential of online voting is discussed, is the risk that employers, partners, or others may force an individual to vote a certain way. This is a genuine risk with online voting but not one which is new or exclusive. The same risk exists with postal voting. There are very few barriers to a malicious actor forcing a partner or someone in care to vote a certain way with postal ballots. With postal voting there is also the risk that voters could evidence and sell their vote. To date, the best workaround for this problem has been the concept of *repeat voting* in which voters are able to vote as many times as they wish but only their most recent vote counts. A voter is also able to cancel their online vote by voting in person on polling day.

This concept depends on online voting taking place over an extended window rather than a single polling day. It also requires the in-person polling day to take place afterwards. This is the same as postal voting in the UK. To an extent, the idea solves the main problems with peer pressure and vote buying – certainly to a greater extent than is the case with postal voting. If someone were to pressure an individual to vote a certain way, the voter could change it back the next minute, hour, or day. Equally, purchasing votes is rendered worthless if the voter can simply change it at will. Finally, being able to undo an online vote by voting in person on polling day is a protection which does not and cannot practically exist with postal voting.

However, *repeat voting*, falls down when it comes to protecting those most vulnerable to peer pressure and manipulation. For voters with housebound disabilities or in care and cannot physically attend a polling station, *repeat voting* is unlikely to prevent their vote being stolen. It is a solution for the able-bodied but not others. Whilst keeping in mind that this still makes online voting more secure than postal voting, it is a problem which must be considered by any government or institution that wishes to introduce an online voting method.

Maintaining audit trails in an online election

Ensuring that a vote cast is the same as the vote counted is of utmost important in all elections. The ability to verify that this is the case is therefore essential to the security of an election and the public's confidence in the result. In a traditional election, this normally involves a series of verifiable interactions with a ballot paper, everything from the voter being issued their ballot paper, to the opening of the ballot box in the count. Can this be replicated with online voting?

[36] Secure Voting, WebRoots Democracy, January 2016.

With online voting, it needs to be possible to audit that all votes are accurately included in the count and that they have not been altered whether by malware on the voter's computer, hackers intercepting traffic between the voter and the webserver, or even corrupt employees at the online voting supplier with access to the stored votes. Some argue that this audit should be undertaken by the voter themselves but given that this isn't the case with the traditional method, it may not need to be so.

One alternative is that this audit could be carried out by a trusted independent body whether they be a private company, the Electoral Commission, or, even, journalists and members of the public. The issue with technology, however, is that to most people its inner workings are akin to a black box. An input is made, something happens, and an output is produced. The argument made by those who are faced with this question is that the inner workings are largely irrelevant and that the output itself is all that matters. Therefore, the focus tends to be on verifying the result itself and given the need for votes to be secret, this verification can only be undertaken by the voter themselves.

Another argument which is often raised in this conversation is that in traditional paper voting, there is no mechanism for a voter to verify that their vote was counted at all, never mind counted correctly. It is therefore argued that a provision that would enable voters to verify that their vote was counted correctly in an online voting option would produce far greater confidence in the process than any audit could ever achieve. Despite this, it would be a mistake to rely on voter verification alone, the inner workings would still, and should still, be subject to an audit. The question is how would this be done and who would undertake it?

Ultimately, this will need to involve the use of external, expert, auditors. Any logs or proofs of the online voting system should be reviewed by auditors before, during, and after an online election. This would represent a significant, but not revolutionary, shift in how elections are administered.

The existing paper balloting system already contains involvement from the private sector across a variety of tasks including ballot printing and delivery, and in, some cases, training of poll staff. The inclusion of the private sector in auditing the security of the voting system would be an extension of this. As with all audits, in any industry, the aim would be to provide reasonable assurance of the robustness of the system.

Contingencies for vote tampering

What should happen if it all goes wrong? Whether an individual vote is found to be tampered with, a handful of votes, or the entire election itself; contingencies must be put in place. Does a voter get to re-cast their ballot? Is an entire election re-run?

This problem is different to the problem of tampering during an election. As mentioned already, *repeat voting* is one mechanism which can be deployed to combat peer pressure or individual vote tampering. Instead, this problem refers to the discovery of fraudulent activity after an election has taken place.

The answer may seem obvious: re-run the entire election. However, this would be a costly decision. Must every single voter re-cast their vote or only those whose vote was tampered with? Would it be fair for some voters to be able to vote again after the election period? Such a decision, to re-run an election due to allegations of fraud, could cause chaos so must be approached with careful consideration.

If vote tampering is proven, there is a question of whether a re-run would be necessary? For example, if it was provably found that X% of votes were inaccurately recorded as a vote for Candidate A instead of Candidate B, could there not simply be a recount? If it was found that Y% of votes were cast by bots or by ineligible voters, could those votes not simply be discounted?

Some have instead focused their attention on minimising the risk of fraud. In Swiss pilots of the technology, they implemented thresholds or limits of the number of votes allowed to be cast online. These are gradually increased as and when other security requirements are met.

The most likely contingency would be that votes would need to be re-run in constituencies where there were a significant number of fraudulent votes. Significant, here, meaning that a result

would have been swung one way or the other. In recent history, an example can be found in the 2014 Tower Hamlets Mayoral election in which the winning candidate was later found to have rigged the vote.[37] He was removed from office in 2015 and the election was re-run with modifications. The key question with online voting is what would these modifications look like?

Ensuring trust in the election outcome

Arguably the most important challenge for online voting is ensuring that the result of the election is trusted and accepted. Even if all of the intricate processes and security measures are robust and uncompromised, false allegations of fraud can eat away at trust and undermine an election. This is particularly the case when that election has taken place online.

With paper voting, this problem is quelled by opening up the vote count process to observers and journalists. Opposing candidates can both watch over officials during the count itself, point out errors and gain confidence in the process. Can the same assurance be replicated with online voting?

Online voting, as with most technology, is seen as a black box to ordinary people. This, therefore, introduces an element of uncertainty into the process. Have the votes been submitted and recorded accurately? The relative openness of the existing paper voting system may be difficult to replicate with online voting. It could be that a new approach altogether must be taken to ensure trust, one which isn't modelled on traditional voting systems. Can we utilise advances in technology to fashion a new, innovative method of garnering trust in an election outcome?

In one way or another, all of these challenges in this chapter are fundamental to building trust in an online voting system. It is important, however, to make the distinction between security and trust as they are two separate things. The online voting system may exceed all expectations and be 100% secure, but if voters or the media cannot or do not understand how it is the case, they may lack trust in the outcome. This will be a critical challenge for any proposed online voting system and one which may require a novel approach.

[37] Tower Hamlets election fraud mayor Lutfur Rahman removed from office, BBC News, April 2015.

user experience for online voting platforms

There is significant cross-over between the accessibility of an online voting platform and its user experience, however, they are distinct characteristics and should be judged as such. The main challenge, here, is to balance the need for a user-friendly online voting platform with the needs for one which has robust security and is accessible to all. If a platform requires various devices or levels of authentication prior to the vote being cast, will this have a negative impact on its uptake? If it is too simple to vote, how can we trust that the legitimate voter is the one who cast the vote? These concerns have to be carefully balanced and considered in the design and implementation of online voting for elections.

Simply building an online voting platform will do nothing to boost turnout and engagement amongst target groups. Without serious thought and consideration into how the platform will fit in with the wider democratic ecosystem, there is a risk of online voting lacking utility. A platform which carries many arduous and stringent security requirements will not be a simpler alternative to existing voting channels. A platform which fails to take advantage of the reach of social media is a missed opportunity. The best online voting platforms should be as beautiful as they are accessible and secure.

To make allowances for creativity, we do not make as stringent recommendations on user experience as we do for accessibility and security. However, there are three key considerations with regards to approaching user experience in online voting. The first is in relation to the balance between security and usability. The second is the opportunity of online voting fostering a more informed electorate. Finally, there are the new challenges which would be faced by this voting channel of online disinformation and political advertising.

Security vs usability

As with any system, there is often a trade-off between security and usability. Some would argue that online voting, itself, is an example of such a trade-off with reduced security in favour of a remote method of casting a ballot. However, it should still be possible to have robust assurances around security and privacy whilst maintaining a user-friendly method of voting. Indeed, some participants in our research argued that voters 'want hoops to jump through' with online voting and would be deterred from voting online if it was made too easy to do so.

It is highly likely that with any online voting platform, will come a requirement for voter identity checks. Any platform without them would likely be dismissed by both governments and voters. This should, therefore, form an essential part of user research in the development of online voting platforms. What level of identity checks would voters be comfortable with and what could the unintended consequences of such checks be? Would it lock some voters out from being able to vote online or can it be achieved in an inclusive manner? It's been well documented that introducing voter ID checks can disenfranchise voters who do not hold formal identity documents.[38] The aim of online voting should be to reduce barriers to voting, not to erect new ones. This will be a key consideration.

Stringent security measures may lead to a higher number of clicks and pages to go through prior to the voter reaching the actual online ballot. Literature and opinion on how much effect the number of clicks has on user experience lacks consensus, however e-commerce sites, in particular, focus on making the process of purchasing a product as straightforward as possible. Whilst this should, perhaps obviously, remain an ambition for any online voting platform, voters will need to be guided step-by-step on how to vote and how to verify their vote. Whether it is through a pamphlet in the post, instructions on-screen, or a three-minute explainer video, this need will be unavoidable.

[38] How does mandatory voter ID disenfranchise the public? Electoral Reform Society, December 2018.

It is important, throughout, to understand that these trade-offs between security and usability already take place in traditional, paper-based voting methods. A polling station could introduce greater security measures to ensure that the correct voters are participating. These could include locked doors, accessible by PIN codes. Poll staff could carry out their own identity checks on voters, scanning their passports and proof of address. Smartphones could be confiscated prior to votes being cast to prevent photographs of ballot papers. Airport-style bag checks and body scans could be introduced to prevent terrorist attacks or other forms of election interference. These measures, whilst possible, do not currently take place. This is because a) the risk isn't deemed high enough to warrant such measures and b) it would erect significant barriers to voting and depress voter turnout. Similar measures could be, but aren't, put in place for the count itself. Body-worn cameras for count staff, quadruple-locked ballot boxes, and bomb-proof count centres could all be measures which increase the security of an election. However, a trade-off is struck and measures are made to be proportionate.

With online voting, the same approach needs to be taken when it comes to this balance. Are proposed security measures necessary and proportionate? Do systems need to be bomb-proof, or do we aim for reasonable assurance? How do these assurances affect voter turnout?

A variety of measures have been implemented or proposed in various online elections around the world. These have included user ID and password credentials sent in the post, hand-held devices similar to card-readers used by banks, and facial recognition technology on smartphones. Any proposal for an online voting platform needs to be assessed on its proportionality, its necessity, and its wider impact on voter participation.

A more informed electorate

One of the great opportunities of online voting is its potential capability to lead to more informed votes being cast at elections. This doesn't refer to 'informed' in the sense of one political party or candidate being better or worse than the other. It refers to voters knowing more about who their local candidate is and what the remit of the candidate would be if elected.

Unlike traditional paper-based voting methods, online voting has the potential to include a wide range of content such as video content or candidate photos. This kind of content is unfeasible or too costly to achieve with paper voting. However, with an online voting platform, it is perfectly feasible (at least technically, if not legally) to allow candidates to upload video content setting out their priorities, copies of their party's manifesto, or, even, answers to a standardised set of questions related to their policy positions.

As for the election, itself, an online voting platform could include content setting out what a certain election is about. This could be an explainer video or simple written content about the role of a Member of Parliament, a Local Councillor, or Mayor. This could help reduce the effect that is often seen at local elections in which voters punish local representatives at local elections by casting votes based on national politics.

Another factor which could be reformed by online voting platforms is the phenomenon of *alphabetical voting* in which voters select candidates who appear higher up on the ballot paper.[39] This effect can particularly be seen in multi-member elections in which the electorate have the option to vote for more than one candidate. One local council candidate with a hyphenated surname told us that they had even been told to drop part of their surname in favour of one which would enable them to appear higher up on the ballot paper. With online voting, there is the potential to work around this effect by randomising the order of candidates on the ballot. To fully understand the effects of this, it would benefit from further research, however with online voting, this idea can practically and affordably be considered in elections for the first time.

These ideas and others can help transform the entire user experience of elections from one

[39] Alphabetical Voting, Newland, 1973.

which is a simple cross in a box to one which is educational, informed, and fair. The capability for voters to understand what exactly an election is about and who is exactly their candidates are, could have the knock-on impact of lifting the quality of debates during elections. Conscious that voters are equipped with more information than ever before, candidates may end up working harder to win the support of the electorate and face a higher level of scrutiny on where they stand on the key political issues of the day.

None of this is to say that any or all of these ideas are desirable, but that they are possible and possible only with online voting. To replicate such ideas in paper voting would be unwieldly, expensive, and impractical. With online voting, the potential exists for the first time and at low cost. Depending on the requirements of the election, these capabilities could add an edge for one online voting proposal over another. Of course, as with any new developments in elections, all consequences should be considered carefully including unintended ones. For example, would an integrated voter advice application create new challenges around security? How would candidate images and videos be standardised? Would candidates with access to higher quality cameras benefit compared to those without access? These are the kinds of questions which should be asked in conjunction during an assessment of novel capabilities.

Political advertising

One of the most important challenges with regards to the user *experience* of online voting platforms is the user *journey*. How does a voter arrive at the online voting platform? Do they arrive there by simply typing in the web address into their browser or do they clickthrough adverts on social media to arrive there? If it's the latter, what does this mean in terms of the law and elections?

In the UK, political advertising is banned around a polling station and it would be inconceivable that postal votes would be sent out by political parties.[40] Whilst it may be the case that postal voters may receive election leaflets at the same time as their ballot papers, this is very different to a voter clicking through onto the election website from a party-political advert on Facebook, for example. Are there new considerations which need to be examined for this highly likely scenario? Little research appears to have been undertaken with regards to this question.

In theory, it could be highly beneficial to have political parties and candidates' direct voters to the online voting page as it could increase voter turnout. Turnout would almost certainly benefit from support from social media platforms themselves promoting an election and this is something which has already been proven. However, are there considerations around the language which could or should be used when doing so? Are there parallels with campaigners handing out election leaflets near a polling station? What would the consequences be of malicious actors directing voters to the page on social media? Are these risks which need to be mitigated, and if so, how?

It may be the case that new legislation is required around political advertising and online voting. Regardless, proposals for online voting should set out plans for how they can ensure voters aren't too heavily influenced by political advertising before they vote. This could be done by placing some distance between the user login and the casting of the vote, or it could be done by providing explainers on the election and the different candidates taking part.

Social media has already been subjected to election interference attempts and there is no reason to believe that these attempts will not continue into perpetuity. Online voting platforms could be affected by this and if it forms part of a voter's user journey, it may influence how they vote. This challenge is one which should not be ignored and is, by no means, impossible to overcome.

These three key areas of consideration will be necessary for any developer of online voting platforms and for any institution seeking to introduce the method for an election. Security trade-offs already take place in elections and a

[40] Polling Stations (Regulation) Bill, UK Parliament, 2007.

balance will need to be struck in online voting. The opportunity to improve the quality as well as the quantity of votes is one which should be given serious attention. The challenges surrounding political advertising and online interference campaigns is one which must be addressed. In general, however, the user experience for online voting can and should start from a blank piece of paper, ensuring that key principles are met, challenges are addressed, and that users are properly involved in the research and design from the very beginning.

the cratos principles explained

Based on the research undertaken as part of this project, drawing upon the experience of users, practitioners, and researchers, we have outlined 33 key principles which should be met by an accessible, secure, and user-friendly remote online voting platform. These principles are explained below.

Accessibility

1. Textual equivalents to visual information

Any images and videos used in an online voting platform should have a textual equivalent which can be read by assistive software or be comprehensible to a user who is vision impaired. This may be relevant for instructional graphics, for example. It is critical that any, and all, important information related to the election is easily accessible for all voters.

2. Compatibility with text-to-speech software

To ensure that the text within the platform is accessible to vision-impaired voters, the platform should be easily compatible with text-to-speech software. This should be considered at the beginning of the design process and properly tested prior to deployment.

3. Enlargeable text and images

All text and images used in the platform should be enlargeable. This will enable voters with poor eyesight to read and understand the content. Whilst text is relatively easily enlarged, it is important to ensure that images do not become pixelated upon resizing.

4. Clear and accessible links

Hyperlinks used in the platform should stand out clearly. For example, failure to bold and underline clickable links may lead to them being missed by voters with low vision or colour-blindness.

5. Inclusive colour schemes

Considering the main forms of colour-blindness (red-green, blue-yellow, and total colour-blindness), a platform with an inclusive colour scheme will be more easily distinguishable for voters who are colour-blind.

6. Capability to be navigable by keyboard

The online voting platform should be navigable by a keyboard and not rely solely upon a mouse or touchpad. This will ensure the platform is accessible for vision impaired voters as well as voters with motor disabilities. Some voters could even be using modified, accessible keyboards which they may depend upon.

7. Capability to be navigable by a single switch device

Some voters with severe physical impairments may rely upon adaptive switches to be able to independently use devices such as computers and smartphones. They come in various forms such as a joystick, a chin switch, and a “sip and puff” switch. An online voting platform which is compatible with adaptive switches could help include some of the most marginalised voters in society.

8. Closed captioning on video content

Ensuring that closed captioning is available on any embedded video content will help improve the accessibility of a platform for voters with hearing impairments. By having closed captions instead of open captions (where the subtitles are burned onto the video itself) the text can be identified and interacted with by assistive technologies.

9. Sign language translations on video content

Including sign language translations on video content will aid voters who have hearing impairments for whom English is not a first language. Having the voting instructions explained in British Sign Language may also help lower barriers to comprehension of the platform.

10. An easy read version of the platform

Creating an easy read version of the platform could help ensure the process is more easily understood by voters with learning disabilities. This if often done already with political party manifestos and election guidance more generally. The same should apply for an online voting platform.

11. A helpline for those requiring assistance

It may be the case that despite assistive measures being designed into the platform, that some users may require further assistance. A dedicated helpline for voters requiring assistance should be set up and clearly displayed.

12. Demonstrable input from users with disabilities in the design and development of the platform

Voters with disabilities should be viewed as the main beneficiaries of an online voting platform. It should, therefore, be designed with their needs in mind from the beginning of the process and not as an after-thought. An online voting proposal which can demonstrate active engagement from these users should rank higher for accessibility.

13. Capability to switch to accessible versions, if necessary, without leaving the main voting application or website

If there is a need to have separate, accessible versions of an online voting platform, these should be made to be easily accessible from the main voting application or website. A requirement to download a different application or to use a different website address may cause undue confusion for voters.

14. Provision of information in alternative languages

There is potential for online voting to help break down barriers to elections for voters who do not speak English as a first language, or at all. Having multi-lingual capability in an online voting platform could enable more voters to participate in elections independently and with greater confidence.

Security

15. Capability for a voter to cast an independent, pseudonymous ballot

A vote should be made untraceable back to the identity of the voter, except by the voter themselves. This is akin to the principle achieved in the existing paper balloting system in which, under specific circumstances, a voter is able to request to see their ballot paper after the vote has been cast. By achieving this principle, a voter is able to cast a secret ballot whilst granting them the opportunity to verify whether their vote was cast and counted accurately.

16. Capability for a voter to verify that their vote was recorded accurately

To ensure that a voter can be confident that their vote has not been tampered with and altered in any way, they should be given the capability to verify whether their vote has been recorded accurately. Whilst, in theory, this is something which is possible in the existing paper balloting system, in practice, it is a level of assurance which voters are not currently able to achieve.

17. A pseudonymised public ledger of all votes cast

Whether centralised, or decentralised (e.g. by local authority area), an online voting system should provide a pseudonymised, public ledger of all votes cast. Using the ledger, three key aims would be achieved. 1) A voter would be able to check that their vote is recorded accurately within the election count; 2) the public (including election officials, political parties, and journalists) would be able to tally the total number of votes themselves; and 3) an audit could be undertaken to provide assurance that voters' choices were recorded accurately. This audit could be carried out by mandating random samples of the electorate to privately verify their vote.

The ledger would act as the single version of the truth, highlighting error as well as accuracy. This principle, whilst representing a significant shift from how elections are run currently, is the best method through which trust in the result can be guaranteed.

18. Capability to verify the identity of the voter prior to casting a ballot

To reduce the risk of an ineligible individual casting a vote, or casting a vote on another's behalf without consent, an online voting system should be able to verify the identity of a voter. The system would not necessarily be required to know personal details about the voter, but it should be able to verify that the correct individual is casting the vote.

19. A mechanism for repeat voting

In order to minimise the risk of voter coercion, an online voting system should allow an individual to change their vote as many times as they wish until the close of the online voting window. This principle, known as repeat voting, would disincentivise the practice of vote-buying and offer an avenue for a voter to amend their vote following instances of coercion by others. Should the individual be unable to effectively cast their intended vote in the online voting window, they should be able to override any online vote, in person, at a polling station on election day.

Whilst this, by no means, reduces the risk of coercion to zero, it offers protections which alternative forms of remote voting (e.g. postal voting) cannot.

20. Contingency plans in case of vote tampering both on an individual and large-scale basis

In case of circumstances where votes are found to have been tampered with, contingency plans should be put in place in order to correct the vote or re-run the election. This is principle is not mutually exclusive to online voting and should apply for existing elections.

21. A mechanism of live-monitoring to detect malicious interference with the system

To help identify malicious interference, a mechanism should exist where election officials are able to live-monitor the online voting system. This capability could help officials notice an abnormal number of votes being cast from a single device. In such a situation, remedial action could be taken before polls close instead of afterwards as is often the case in paper-based elections. The mechanism, however, should never link voters to their choices.

22. A mechanism for independently auditing every process, interaction, and instruction

Nothing related to the workings of an online voting platform should be kept in the dark. In order to gain assurance that the system is working as it should, there should be a mechanism for every process, interaction, and instruction to be independently audited. This will not only build confidence in the system, but it will help officials to identify what went wrong in cases of failure.

23. Encryption and subsequent deletion of voter records and personal data

To minimise the risks of voter details being compromised, voter records and personal data should be encrypted. Only the voter should have the capability to decrypt their vote. As a minimum, the deletion of voter records should take place after the window of appeal (to dispute the vote) has closed. This mirrors existing paper-based systems in which voter records and ballot papers are kept for a prolonged period following the election, before being destroyed.

24. Contingency plans for interruptions in the availability of the platform

Should an online voting system be unexpectedly taken offline (e.g. following a successful distributed denial of service attack), contingencies should be put in place to allow voters to participate in the election. This could involve extending the online voting window by the same length of time it was offline or, even, issuing emergency postal ballots.

25. Guidance to inform voters about how to securely cast a ballot

An online voting system should provide clear and understandable aids to assist a voter to accurately, securely, and secretly cast a ballot. Guidance should also be provided to inform a voter about how to verify their vote and what to do if they are subjected to coercion.

26. Capability for an online vote to be overridden by a vote cast in person

Any online vote cast by an individual should be overridden by a vote cast in person. This offers a form of protection against voter coercion and reduces the risk of an illegitimate vote being recorded. This principle also acts as a contingency in circumstances where an online voting system is found to have been compromised.

27. A commitment to share the platform's source code with relevant electoral administration staff and independent auditors

A secure online voting platform is one which is highly transparent. This transparency should apply to the source code. In order to allow for independent examination, the source code of an online voting platform should be shared with the election authorities and the appointed auditors. This opens the door to procedures such as white hat hacking, whilst minimising the risk of malicious actors silently identifying vulnerabilities. Should an online voting system be designed by the private sector, as opposed to the public sector, this principle will help protect developers' intellectual property and ensure that a strong commercial market can be fostered around online voting. A weak commercial market may lead to weak online voting systems.

User experience

28. As few as clicks as necessary for a voter to cast a ballot

To ensure that online voting does not become a burdensome method of voting, the platform should be designed in such a way that does not require a voter to click-through an excessive number of pages.

29. Capability to include images and information on individual candidates

An online voting platform should have the capability to include photos and information on candidates. This information could be a link to their party's manifesto or it could even be a video pitch to voters. This will help voters to better identify their candidate(s) of choice.

30. Capability to include key information about the election

In order to help voters understand the nature of an election, an online voting platform should include clear information about the election and the role of elected representatives. This will help avoid misunderstandings around a voting system (e.g. first-past-the-post) or confusion surrounding the role of a local councillor and an MP.

31. Social media integration

To help increase voter turnout in an election, the online voting platform should promote to voters the option to share details of the election with their friends on social media. This could look similar to Facebook's 'I Voted' function which studies have found to have had a positive impact on voter turnout.

32. Randomisation of candidate positions on the ballot

To minimise parties or candidates gaining an unfair advantage in elections by virtue of being placed higher up in a ballot paper, the order of candidates in an online voting system should be randomised for every voter. To ensure that this randomisation does not cause undue complication for a voter in finding their candidate of choice (particularly in elections with a large number of candidates), an option to search for a particular candidate could be provided.

33. Capability to cast and verify a vote on the same device and application / website

Online voting systems which enable voters to be able to verify their vote on the same device and application will rank higher for user experience than those which require a voter to have more than one device.

our proposed rating framework

Our proposed rating framework assigns weights to each of the 33 *Cratos Principles* and provides a triple letter rating of online voting platforms; indicating how accessible, secure, and user friendly it is. Grades are scored from A – E. A rating of AAA would indicate that the platform is highly accessible, secure, and user-friendly.

The framework also provides an overall score out of 220. Principles related to security carry the heaviest weighting of 100, with accessibility and user experience having total points of 85 and 35 respectively. Principles deemed to be the most critical carry a greater weighting.

This framework is not exhaustive and should serve as a useful tool for the initial analysis of an online voting proposal. Whilst some of these criteria are most relevant for statutory national elections, it should also be useful for private organisations wishing to undertake internal elections. For example, a private members organisation running a low stake internal poll may be satisfied with a low security rating as long as the user experience rating is high. For national elections, proposals should aim to score highly in all three categories.

Ratings scale

Criteria	Score				
	A	B	C	D	E
Accessibility	68-85	51-67	34-50	17-33	0-16
Security	80-100	60-79	40-59	20-39	0-19
User experience	28-35	21-27	14-20	7-13	0-6

Weightings for accessibility

Principle	Maximum score
Textual equivalents to visual information	5
Compatible with text-to-speech software	5
Enlargeable text and images	5
Clear and accessible links	5
Inclusive colour schemes	5
Capability to be navigable by keyboard	5
Capability to be navigable by single switch device	5
Closed captioning on video content	5
Sign language translations on video content	5
An easy read version of the platform	5
A helpline for those requiring assistance	5
Demonstrable input from users with disabilities in the design and development of the platform	20
Capability to switch to accessible versions, if necessary, without leaving the main voting application or website	5
Provision of information in alternative languages	5
Maximum score	85

Weightings for security

Principle	Maximum score
Capability for a voter to cast an independent, pseudonymous ballot	5
Capability for a voter to verify that their vote was recorded accurately	5
A pseudonymised public ledger of all votes cast	20
Capability to verify the identity of the voter prior to casting a ballot	5
A mechanism for repeat voting	10
Contingency plans in case of vote tampering	15

both on an individual and large-scale basis	
A mechanism of live-monitoring to detect malicious interference with the system	5
A mechanism for independently auditing every process, interaction, and instruction	5
Encryption and subsequent deletion of voter records and personal data	10
Contingency plans for interruptions in the availability of the platform	5
Guidance to inform voters about how to securely cast a ballot	5
Capability for a vote to be overridden by a vote cast in person	5
A commitment to share the platform's source code with relevant electoral administration staff and independent auditors	5
Maximum score	100

Weightings for user experience

Principle	Maximum score
As few as clicks as necessary for a voter to cast a ballot	5
Capability to include images and information on individual candidates	5
Capability to include key information about the election	5
Social media integration	5
Randomisation of candidate positions on the ballot	5
Capability to cast and verify a vote on the same device and application/website	10
Maximum score	35

In each category, some principles are weighted more heavily than others due to their level of importance. For example, *demonstrable input from users with disabilities in the design and development of the platform* is critical to the accessibility of an online voting platform. With a maximum point score of 20, developers are incentivised to involve voters with disabilities as much as possible in order to obtain a higher rating. Amongst the security principles, *a pseudonymised public ledger of all votes cast* is ranked the highest due to the impact it could have on boosting the trustworthiness of an online election. For user experience, *the capability to cast and verify a vote on the same device and application/website* is weighted slightly higher due to the impact that having to verify the vote on separate devices may have on the likelihood of a voter verifying their vote and on the voting experience in general.

This framework, however, should be used as a helpful indicator of the robustness of an online voting proposal in conjunction with the many challenges, questions, and considerations raised throughout this report. It can be used as a method to help assess an online voting proposal, a trial, or for the evaluation of real-world implementations.

acknowledgments and methodology

We are extremely grateful to everyone who has shared their expert insights as part of this project and to the Paul Hamlyn Foundation for supporting this research.

We are especially grateful to Professor Kevin Curran, Professor Feng Hao, Dr Garfield Benjamin, and Dr George Theodorakopoulos for reviewing the report and providing feedback on the *Cratos Principles*.

In addition, this report would not be possible without the invaluable support of the WebRoots Democracy team, particularly Laura Deslandes, Rachel Fielden, Maya Fryer, Fahmida Rahman, Khadija Said, and Tess Woolfenden who assisted with key research activities throughout the project as well as Milton Brown and Ben Pearson who helped review final drafts.

Individuals who fed into this research during our roundtables, forums, and interviews held across Birmingham, Edinburgh, and London are listed below.

- John Abbott (Yoti)
- Sonya Anderson (Smartmatic)
- Dr Garfield Benjamin (Solent University)
- Ian Brightwell (Electoral Commission, New South Wales)
- Professor Kevin Curran (Ulster University)
- Julie Dawson (Yoti)
- Paul Docker (Cabinet Office)
- Maria Fernanda (Smartmatic)
- Dr Rowanne Fleck (University of Birmingham)
- Dr David Galindo (University of Birmingham)
- Professor Feng Hao (University of Warwick)
- Nick Hatton (Royal Holloway, University of London)
- Simon Hearn (Electoral Reform Services)
- Dr Grammateia Kotsialou (King's College London)
- Ivo Kubjas (University of Tartu)
- Dr Ian Levy (National Centre for Cyber Security)
- Ruth Maguire MSP (Scottish Parliament)
- Dr Syed Naqvi (Birmingham City University)
- Kasimir Rantzau (University of Westminster)
- Dr Luke Riley (King's College London)
- Omari Rodney (Yoti)
- Samuel Rowe (Oxford Internet Institute)
- Professor Mark Ryan (University of Birmingham)
- Dr Muntadher Sallall (University of Surrey)
- Jeff Stern (Votem)
- Mike Summers (Smartmatic)
- Lucky Tavag (Votem)
- Liz Ure (Scottish Government)
- Joe Wadsworth (Electoral Reform Services)
- Thom White (Yoti)
- Dr Bingsheng Zhang (Lancaster University)

Methodology

The research for this project took place between 2018 and 2019. Following a period of desk-based research, reviewing existing literature and building upon our own institutional knowledge (dating back to 2014), we organised a series of events, roundtables, and expert interviews in Birmingham, Edinburgh, and London. These events took place at the University of Birmingham, the Scottish Parliament, the UK Parliament, and TechHub London. Participants for our roundtables were recruited via a combination of personal invitations and open calls.

This version (v2) has been updated to correct an error of omission in the ratings framework.

WebRoots **Democracy**