# Remote E-Voting: More than a Technical Challenge

**Kyra Mozley**

Royal Holloway, University of London

Kyra.Mozley.2020@live.rhul.ac.uk

March 2021

**Abstract -**

**This paper will discuss the issues countries face beyond the technical challenge of implementing a secure electronic voting system. We start by exploring the history of national elections, the system's current flaws, and why moving to electronic-based voting would be beneficial. We look at the requirements for an e-voting system; we discuss the challenges nations face in developing trust, acceptance, and creating a system with usability in mind, allowing voters to feel secure in adopting this new technology. Lastly, we turn to look at the implementation of e-voting in Estonia and discuss whether it could be done as successfully in the UK.**

## 1 Introduction

Everything we do is now online, and information technology has made things more efficient, convenient, and accessible. But why has digital innovation not been applied to the UK's voting procedure? Manual voting has several obvious drawbacks: inaccuracy in ballot counting, inconvenience, and the delayed election results announcement. [1] E-voting has attracted considerable attention over the last decades, often proposed as the answer to increasing voter turnout. While some people want to modernise our election process, we wish to outline that introducing e-voting is a complex problem that needs attention from many disciplines. Many scientific papers have been written on this topic, primarily covering the technical issues surrounding the security of e-voting. Here we wish to bring to light sociotechnical issues that developers and governments must consider from the start if they wish to revolutionise our traditional voting procedure.

This paper is organised as follows; we begin by defining what elections need, what remote e-voting entails and the potential benefits. Next, we discuss three non-technical issues designers must consider when implementing these systems. That is those of usability, trust, and everyday security. We then turn to look at how Estonia had managed to implement e-voting considering these issues. Lastly, we argue that the UK could not achieve remote electronic voting with the same success.

## 2 Background Knowledge

### 2.1 Election Requirements

Elections seem to have two, almost somewhat contradictory, requirements: anonymity and verifiability. [2] Verifiability allows a voter to be sure their vote counts, whilst anonymity guarantees you cannot link an individual to their vote. Even though voting has been considered to date back as early as the Roman Empire [3], the concept of anonymously voting is fairly new; Australia first practised it in 1856. [4] However, nowadays, the secret ballot is seen as compulsory in all Western democracies. [4]

There has been an attempt in the literature to create a list of requirements that designers need to consider when designing voting systems. [5, 6] These include, but are not limited to, accessibility, availability, integrity, robustness, and uncoercibility. Ultimately these requirements ensure that the elections are meaningful and therefore contribute to our democratic process. Consequently, if we wish to reform the traditional paper ballot without obstructing the current security, privacy or legal requirements of elections, we must fulfil these conditions. Failure to do so could result in a lack of trust in the result, provide the population with no incentive to vote, or foster societal dysfunction. [2, 7]

### 2.2 What is e-voting?

The UK's current polling procedure is that of a paper ballot voting system. An individual attends a polling station, marks their choice of candidate on the provided paper, and then puts it in the ballot box for the vote to be manually counted at the end of the day. [8] An alternative approach that has gained much attention in the past decades is electronic voting. Electronic voting, or e-voting, is defined as using computers or computerised machinery to cast votes in an election. [1] There are two types of electronic voting systems. The first, poll-site electronic voting systems (PEVS), is where an individual physically goes to the polling station and uses a direct recording electronic machine to record their vote. [5] Whereas the second type, remote electronic voting systems (REVS), allows a voter to vote over the internet without

being physically present in a supervised environment. [3] This paper is concerned with challenges implementing the latter, but issues presented should also be considered by those designing PEVS.

### 2.3 Potential Advantages

People believe that e-voting will be able to offer many benefits compared to our current election system. These advantages include the potential to increase voter turnout [9] since e-voting will remove the barrier of distance between those eligible to vote and the polling station. [10]

However, the concept of remote voting is not new. The postal vote as an alternative to an in-person ballot is an increasingly popular choice. In the UK's 2017 general election, the percentage of people who voted by postal vote was 21.7%, up from 12.7% twelve years earlier. [11] Postal voting may offer similar benefits to e-voting [12] and allows us to fit voting around our busy lives, making the process more convenient, so perhaps this could extend to REV. Nevertheless, in the 2005 election, 33% of nonvoters claimed a circumstance on the day prevented them from voting. [13] Postal votes do not prevent against last-minute conflicts as it requires advanced planning. Therefore, since e-voting offers an individual the opportunity to vote from anywhere, requiring very little time, it could increase voter turnout. E-voting could also increase the efficiency and accuracy of the electoral system [14], and lower the cost of elections. [9] However, many of these advantages have been dismissed or disputed due to a lack of empirical evidence. [14]

We do everything online; we bank online, shop online, and now due to the pandemic, we learn online. Therefore it seems inevitable that it is only a matter of time before we vote online too. Whether or not e-voting would provide the claimed benefits is not of concern here. Designing a system that meets all the requirements outlined in section 2.1 is a difficult technical challenge, but instead, we focus on issues beyond the technical. We wish to highlight the sociotechnical challenges if we adopted electronic voting.

## 3 Non Technical Challenges

The design of REVS concerns many stakeholders from a broad range of disciplines. Academics from various backgrounds, such as computer science, psychology, economics, and politics, have all researched designing e-voting systems. [13] In this section, we focus on issues that lie in the intersection of these disciplines. Firstly, we discuss usability, which is concerned with the interactions between human and computers. Next, we turn to issues around trust and how trust can either inhibit or facilitate success. Lastly, we look at everyday security, which is concerned with the continuation of an individuals routine and how practices are felt.

### 3.1 Usability

Voting is rare in terms of design since it needs to be usable by almost every citizen. Whether they are 18 or 80, disabled, illiterate, or do not have English as a first language, every eligible voter needs to be able to use the voting system. In addition to meeting the needs of the whole population, designing a voting system is problematic since, as a task, it infrequently occurs, meaning users do not have the opportunity to practice performing it. Most technologies benefit from learnability and memorability; when we get a new device, we may be unsure how to use it, but repeated exposure makes using it second nature. [15] Voting does not possess this advantage. People's first encounter with a voting system is the first time they vote, and there is little assistance provided, as well as social pressure to do it without help. [16] Lastly, in a voting system, accuracy is critical; Designing a voting system without usability in mind can introduce problems that not only affect an individuals satisfaction with the process, but can threaten the credibility of the whole procedure, thus undermining democracy. [17]

First, we must define what usability means. ISO and NIST [18, 19] define usability as *"a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users performing specified tasks with a given product"*. Putting these three components in the context of voting, we create three criteria for investigating usability: [20]

- *Effectiveness* The accuracy and completeness in which an individual casts their vote
- *Efficiency* The completion time for a voter to mark their ballot
- *Satisfaction* The comfort and acceptability of the voting system by users and others affected by its use

However, measuring the first aspect of usability concerning voting systems is challenging. We typically measure effectiveness through observing participants, but this would break the secrecy and privacy we require for elections. [20] Providing the subjects with voting instructions and intent cards (i.e. a 'fake' election) have been used to solve this issue [21, 22, 23], but this could generate less meaningful results. Another problem in measuring usability is that it may not reflect the real election day scenario. Polling occurs in a setting that can pressure voters to perform the task quickly and appear competent, which may leave the individual

feeling flustered and likely to lead to more errors. [17] Therefore, designers need to consider how to measure the usability criteria accurately whilst keeping the scenario realistic. If we fail to implement a usable electronic voting system, it could lead to mistakes when voting. These resulting errors mean the voter's true intention was not accurately recorded, thus impacting the election's integrity, an essential requirement we identified in section 2.1. [20]

Furthermore, the perception of an electronic voting system can potentially impact an individuals intention to vote. Yao and Murphy [13] identified five characteristics of REVS that independently influence voters intention to vote using the system; these are availability, ease of use, mobility, privacy, and accuracy. Ease of use and accuracy fall within our definition of usability. Therefore, if a system were deemed unusable, or people believed it was not recording their votes accurately, it would negatively impact an individual's intention to vote.

E-voting has the potential to exclude large groups of the population from participating in the election, which would have a devastating impact on democracy. [14] There is a belief that younger people are better at performing computer tasks than their older counterparts [16]. So older generations may feel unsure or unfamiliar with the new system. Additionally, whilst testing the usability of smartphone voting systems, Campbell [24] found that those unfamiliar with smartphones and those with the lowest education levels were disproportionately affected in performance. We cannot ignore that the digital divide is still very much an issue in the UK. In 2018 10% of adults were described as 'internet non-users' [25]. Fundamentally we should not assume the whole population has equal access to e-voting. [26] Therefore, there is potential that REVS could benefit the younger, highly educated members of society.

The 2000 US presidential election served as a reminder that system design failure in the election process can alter election outcomes. [27] The arrangement of names on Florida's notorious butterfly ballot led voters to cast a vote for a different candidate to the one they intended. [15] The controversy that followed the results of the election meant that, as a result, academics began researching the usability of voting systems. [6] And in 2002, the US government passed the Help America Vote Act (HAVA), which mandated equal voting access for all citizens and required states to update their voting systems. [28] Most states adopted a PEVS, using direct-recording voting machines (DREs) for elections. DREs were innovative systems, which should have minimised voting errors.

However, testing of these machines showed that citizens can still make errors using them, up to 9% in some cases [24] and these inaccuracies are large enough to alter the outcome of a close election, like that of 2000. [17] Additionally, visually impaired individuals still face challenges using these e-voting systems. [29] Illustrating that despite the HAVA promising to provide equal access, the machines have failed to meet accessibility needs, and those with disabilities struggle to vote independently, privately, or successfully. [30] In 2012, almost a third (30.1%) of disabled voters reported challenges with voting, compared to 8.4% of voters without disabilities. [31] The voter turnout for those with disabilities was also lower than those who did not identify as disabled. We determined that poor usability can influence a persons intention to vote; perhaps after years of systems that have not considered their design needs, these members of the population have been disenfranchised to vote.

While DREs are fundamentally different from the REVS we consider, both types of e-voting offer similar usability opportunities. Therefore, the poor implementation of DREs across the US should highlight both the importance of usability in voting design and the need for more consideration and research into meeting the populations' needs with such systems.

We argue that if the REVS designers implement the system well, it could be more usable than our current paper ballot system. E-voting has the potential to do things that paper cannot, such as allow an individual to change the font size or the language of the system or enable disabled users to customise their experience. [16] For example, blind individuals have suffered confusion with the current paper ballots since the braille text with party names could be above or below the ballot.[9] REVS offers these individuals an opportunity to use screen readers on their own devices, allowing them to vote with confidence and alleviate this confusion. Overall, allowing users to use their own devices to vote exploits the training the individual has already undergone to become familiar with the device, in turn reducing errors. [24]

Furthermore, an electronic ballot design could prevent voters from making mistakes in a way that paper cannot. In the UK's 2017 general election, over 18,000 individuals voted for more than one candidate. [11] Whilst some of these would have been people intentionally spoiling their ballot, we cannot overlook that some may have been a result of error due to uncertainty in how to vote. [28] REVS can be programmed to ensure you can only vote for one candidate, obstructing users from making this mistake, and so would increase effective voter turnout.

Lastly, we must consider the assistance available with REVS. A trial of REVS in Arizona left telephone help desks overwhelmed with calls. [32] If e-voting is to provide claimed benefits of reduced costs and increased efficiency of the voting process, voters need to be able to

understand how to vote without assistance from another human. E-voting can allow designers to utilise instruction videos or animations to assist the voter in casting their ballot. [9] This could therefore reduce the confusion around ambiguous text instructions.

To conclude, any e-voting system's usability needs to be thoroughly studied since it can impact voters' intentions to vote and the election results themselves. Designers should consider human factors research early on and reach out to all different groups within the population to ensure the systems meet their usability requirements. Whilst we cannot rely on training and learning to mitigate usability issues, designers can take advantage of the electronic medium to assist the user with the electoral process and prevent errors in the balloting.

### 3.2 Trust

The next non-technical challenge we turn to is that of developing trust around the e-voting system. Not only does the system need to be trustworthy, meaning that the system will not lose or tamper with the ballots, but we also need to convince voters to trust that the system really does have these properties. [5] If there were a lack of trust in REVS, people would not want to use the technology, meaning e-voting may not increase turnout. [33] Public trust is fragile; once trust is gone, it can be difficult to regain. Trust is also necessary for a system to be successful [34] therefore, we must consider it as a critical issue for designers to address. Additionally, if a REV result was very close, its trust may be called into question. Traditionally, if an election is close, a recount of the paper ballots is called to assure citizens of the result; with REVS, we would lose that reassurance, meaning allegations of fraud may arise.

We define trust as a decision made by an agent (the trustor) to rely on another agent (the trustee) to perform a given action. [35] In this case, for a voter to trust REVS they have to rely on the system to count their vote accurately, only allow those eligible to vote to do so, not be subject to interference, and many more criteria. As part of this assessment on whether to rely on the agent, a trustor will establish the risks and decide whether or not to accept them. [34] Hence before we can trust a system, we have to understand the risks involved with its use. But, applying this to e-voting, we are presented with a challenge. For our current paper ballot system, the user can form a mental model of how (they think) it works to weigh up the risks. However, REVS are much more complicated due to the complexity of equipment, so understanding the process's risks will be challenging, making developing trust harder. Furthermore, some of the systems used for implementing e-voting have been proprietary or remained secret [34], meaning this lack of transparency makes it almost impossible to make a judgement about the risks.

Interestingly, systems do not need to be secure for users to think they are; individuals will use insecure systems if they believe they are secure. [33] This highlights that, as well as developing a trustworthy system, we need to focus on perceived trust. One of the features that can lead to increased perceived trust is usability. [9] In the last subsection, we saw the importance of designing a usable system with relation to a user's intention to vote. Now we develop a deeper understanding of why. If usability can influence whether or not a person trusts the system, then in the event the system was designed poorly, the user will not be comfortable using it, developing distrust and, in turn, a lack of willingness to use it.

Trust in technology is not sufficient; we also need to consider the social context around developing trust. Oostveen [33] showed that more than the security of the voting system itself could influence the perception of trust, extending beyond the technical to include the organisers' reputation, mass media, convenience, and opinions of friends and family. Furthermore, there is a relationship between trust in government and trust in voting; an increase in trust in the government increases public confidence in the electoral process [34] and also fosters acceptance of e-voting technologies. [14] Therefore, to introduce REVS, it must be when the population has a firm belief in the political leaders if we wish it to succeed. Additionally, with trust established in government, the individual is not as concerned with the verifiability of the election system, [36] which solves the issue of e-voting systems being too complicated for the user to understand; they instead put their dependency in the government rather than the technology.

Ultimately, developing trust around e-voting is essential because voters could place the processes legitimacy into doubt without it. REVS requires the population to form new trust models, and so the government needs to develop the system to promote voters' perceived trust.

### 3.3 Everyday Security

The last issue we turn to is that of the everyday. Everyday security refers to the lived experiences of security practices; it invites us to recognise the more mundane, ordinary routines, and the day-to-day. [37] These routines that individuals create provide stability in their lives; the knowledge of what their day will look like allows them to 'go on'. We should see everyday security as a story of enablement rather than just protection from threats. [38] Concerning voting, we should consider the practices the individual may already have in place; the actions around the action of voting. Elections are a ritual,

[14] therefore, we suggest that introducing e-voting would disrupt the rhythm on which people vote, threatening their everyday security and leaving the individual feeling insecure.

The act of going to the polling station forms part of this election day ritual. It is traditional and well established as part of the electoral process, and this familiarity leads the system to be accepted and provides the voter with confidence. [34] If we were to introduce REVS, the voter would no longer travel to a polling station and instead vote from the comfort of their own home. This unfamiliarity may contribute to the voter rejecting e-voting since voting would no longer *feel* the same. Furthermore, voting is a solemn act, so we need to be thoughtful of the potential of this aspect disappearing if we introduced REVS. [9] Perhaps if people voted from their smartphone, they would not consider the election process as seriously as they currently do. Therefore, when implementing an e-voting system, we need to consider the voter experiences, feelings and how they manage the process [37] since REVS may threaten how voting is perceived. To maintain the familiarity of the traditional election, designers could layout the REVS ballot similarly to that of the current paper ballot. [34] This familiarity would act to provide some confidence to the voter in this new uncertain environment, making them feel more secure in the process.

However, one could argue that due to the fact elections occur infrequently, perhaps they already disrupt our routines, especially for first-time voters who do not have an election ritual. The UK typically holds general elections every five years (although they may be triggered earlier by parliament). This long gap between voting might mean the process interrupts individuals day-to-day, so they may feel negatively towards voting if it is not compatible with their daily routine. REVS offers an opportunity to create minimal disturbance to an individuals routine, as they can vote from any location on their personal device at a time of day that suits them best. Hence, e-voting brings more automaticity to voting. [39]

Overall, we must reflect on how voters will feel about new voting procedures, as well as how it interacts within their daily lives. We suggest that e-voting may threaten the practices and rituals individuals have created around the act of voting. On the other hand, REVS offers the potential to enable those who view the current electoral process as an interruption of their day-to-day, especially for first-time voters.

# 4 The Case of Estonia

In 2005, Estonia became the first country to allow remote e-voting in elections, and in 2007 introduced it as an option for its parliamentary elections. [40] Since its introduction, the amount of people using e-voting has continued to increase; in their 2019 parliamentary elections, 43.8% of participating voters chose to vote through their i-voting system, an increase of 13.3% from the last parliamentary election four years earlier. [41]

The system was made possible due to the existing implementation of their national ID cards, which had been a legal form of authentication since 2002. [40] Originally, the voter would use a smart card reader with their device to verify themselves. However, in recent years an additional option of a mobile-based authentication was made. Online voting for the election opens during the advance voting period, which lasts for six days, from the tenth to the fourth day before election day. [42] A key feature of the i-voting system, and an attempt to meet the uncoercibility requirement of voting, is the ability to revote during the advance voting period. A voter can change their vote on the i-voting system as many times as they want and have the opportunity to cast a paper ballot at the polling station during this advanced period (where the paper ballot takes the highest priority). [43] To be able to check whether an individual has cast an in-person vote as well as an internet vote, there must be a link between the (encrypted) votes and a voters identity. Whilst there have been concerns raised around the technical security of the i-voting system [44], officials do not share the concerns and instead praise the country on its innovative efforts. We now discuss how Estonia's i-voting system relates to the three non-technical challenges introduced in the last section.

## 4.1 Usability

We previously highlighted the importance of considering human factors research to ensure that the system was usable by different groups within the population, and also the opportunity of e-voting to be more usable than the traditional ballot. We argue that the uptake of e-voting is a clear indicator that their system is usable. In addition to a large number of the population opting to vote this way, what is interesting is that there appeared to be no significant skew in the age distribution towards the younger generations.[45] Implying that Estonia has managed to address concerns around older generations not welcoming e-voting. However, they did not manage to meet the needs of distinct other demographics. Around 15% of Estonian's have Russian as their first language, but the voting software was only available in Estonian. [43] Most native Russian speakers opted to vote in person rather than use the i-vote system, indicating using the software presented a barrier for the native Estonian Russian speakers. [45]

Next, using the smart card system to vote meant that the designers were exploiting the training individuals had already undergone in other e-services offered at the time.

Consequently, the user would not be overwhelmed when using it to vote for the first time since the process was familiar. However, during the first national election, those who chose to vote traditionally claimed a hardware barrier, rather than an attitudinal one, prevented them from e-voting. [45] Having to own a smart card reader, a computer, and internet access presented obstacles to voting, and accounted for more than half of the reasons why individuals did not use the i-voting software. We argue that this statistic would be significantly lower today; in 2002, during the introduction of smart cards, only 48% of the Estonian population had internet access. [46] Whereas today that figure stands at around 90%. [47] So, although we cannot ignore issues the digital divide poses, more and more individuals now have internet access, and Estonia has tried to reduce the barrier that is owning a card reader poses by introducing authentication through their smartphone app.

Lastly, e-voting has managed to make the process of casting ballots superior to a paper ballot by preventing users from making errors as it does not allow over or under-voting. [43] Also, the voter receives on-screen confirmation so that they can be sure they cast their vote. In addition, the option to revote on the i-voting software mitigates the possibility of voting for the wrong party.

Overall, it appears that the roll-out of the i-voting system considered usability strongly during the design process, with no large failures reported. However, it may have marginalised some groups (such as those without Estonian as their first language) within the population.

### 4.2 Trust

Trust in the government was a contributor to the success of the introduction of e-voting in Estonia, and their president even advises countries to "build trust before introducing e-voting". [48] We previously stated that trust in the government would increase public acceptance of e-voting technologies, and Estonian's have, on average, higher trust in their government than other EU member states. Besides, the government constructed its e-governance infrastructure based on the idea that citizens trusted them. [49] Since Estonia already offered many other services digitally when introducing e-voting, their citizens would have had more confidence in the government to deliver this service than if they had not. Avgerou [50] stated that E-voting was likely to be trusted if established with other initiatives to create a positive digital culture in the country, and Estonia, often referred to as a digital pioneer, is a clear example of this.

The transparency of the i-voting system was an essential design requirement. The system's process's and management were made available to the Organisation for Economic Co-operation and Development (OECD), all political parties, and accredited observers. [43] They gave those individuals a chance to review all documentation, the software's source code, and all procedures in place. Large parts of the documentation and source code have also been made publicly available. This openness of the i-voting system had a notable impact on building confidence and trust. [51]

Another aspect of the system that increases public trust in the process is the ability for vote verification. An individual verifies their vote was delivered using a smartphone application to scan the QR code displayed on their computer's voting software. [51] When this feature was released, a media campaign accompanied it, raising awareness of how to engage with it. Nevertheless, they found only around 3% of their voters actually choose to verify votes.[51] We stated in section 3.2 that trust in government reduces citizens concerns around the verifiability of the system, and this low uptake of vote verification supports this argument. Although, the option to verify their vote generally increased public confidence in the system.[51]

Despite the transparency of the i-voting system, there was a lack of qualified individuals who could understand the process and provide adequate feedback. [43] The electoral committee offers a two-day course on the system's implementation details for those citizens who wish to become observers, but attendance is low. Attendees have reported of an overload of information, and the majority do not complete the course. [51] We previously stated that the complexity of REVS would be an issue regarding trust since it is inherently harder to understand the risks. So perhaps more needs to be done to address the level of technical details provided to enable more individuals to engage with the electoral process.

### 4.3 Everyday Security

In section 3.3, we suggested that electronic voting could disrupt the rituals individuals had created around the traditional voting procedure. But what is interesting to note here is that Estonia is a relatively new democracy, restoring independence in 1991. Hence, they are less likely to see the voting process as traditional or associate familiarity and routine with it. [34] This lack of established practices around voting may have contributed to the successful uptake of the i-voting system. We said that the everyday must consider the mundane, day-to-day experiences and how these are felt. Using smart cards to enable citizens to vote exploited the fact that some citizens had already adopted these technologies into their everyday practices, thus creating less tension when using them to vote. On top of that, the voting application design

stayed unchanged within the first six years of launch [40] providing a sense of stability to their voters. What's more, since Estonia has always led the way in adopting innovative technologies, [51] citizens may see it as part of their identity and so be eager to introduce these new practices into their lives.

It was believed that lowering the barriers to voting would lead to a higher voter turnout. However, the extent to which Estonia achieved this is questionable since the turnout has remained relatively the same. [12] Instead of getting more people to vote, they just changed the voting habits of active voters. But, relating to the everyday, they found that switching back to paper ballots after using the i-voting system was rare. So we conclude that the system did not provide users with friction around their current voting rituals. Moreover, the introduction of e-voting supported those who vote 'from time to time', since around 11% of online voters stated that they probably would not have, or definitely would not have voted if e-voting had not been an option. [45] Thus endorsing our earlier theory that voting itself disrupts our everyday since it occurs once every few years and challenges our routines, so this increased convenience creates fewer barriers for its use, enabling more people to vote.

Overall, once people began online voting, they continued to do so showing that it can easily become part of ones voting ritual. Moreover, the nation's use of existing technologies and digital approaches likely lead to the acceptance of e-voting, since technology formed part of peoples everyday practices.

## 5 Discussion

After discussing the successful implementation of remote electronic voting in Estonia, we turn to discuss the potential of e-voting in the UK. In section 2.3, we stated that around one in five people voted in the 2017 general election via postal vote; this statistic has been increasing since its introduction as an option to the general public in 2001. This rise of individuals opting for the remote voting option indicates that there potentially is a demand for e-voting. Furthermore, perhaps the coronavirus pandemic has highlighted a need for it. The government postponed the local and mayoral elections that were due to occur in May 2020, whereas if REVS were an option, this delay might not have been necessary. The US state of Wisconsin held their primary elections during their lockdown, and as a result, dozens of voters and poll workers became ill after. [52] So maybe these old methods are incompatible with our *new normal*. However, we argue that the achievement of Estonia's i-voting system would not apply to the UK. Firstly, the lack of nationwide digital identification presents a large obstacle. Several trials of e-voting have occurred in the UK, and these tended to require the voter to log on using an ID and password. [53] But surely this is not enough to verify the individual voter and makes it easier to conduct operations such as vote-selling since one could transfer their details to someone else. In turn, violating the requirement for each person only to vote once. There have been allegations of postal fraud in the past, and whilst these are generally on a small scale, a poor verification system for REVS could lower the barrier for vote selling and election fraud. There would also be concerns raised if we required people to use identifiers such as driving licenses or passports since not everyone owns them and they can be costly to obtain, thus potentially creating a barrier for the poorest in our society to vote. Therefore, without a national ID infrastructure like Estonia, we must put more thought into addressing the identification challenge in this country.

Beyond the lack of technical infrastructure to implement e-voting, the UK has a more prominent issue; lack of trust. In the latest YouGov poll, only 27% of people said that the prime minister was trustworthy. [54] We have stressed the importance of trust in government regarding delivering e-voting. Hence, until we restore public trust in the government, a reform of the electoral process seems out of reach. Whatsmore, we flagged reputation as a factor in forming an individual's perceived trust in the system. However, our government does not have a successful reputation for large projects; e-voting is a big project, and big projects often fail. In the UK, 7 out of 10 government IT projects have failed. [55] We only have to reflect on the last year with the chaotic delivery of the contact tracing application, or the disastrous rollout of Universal Credit over the last decade to see why the government's reputation for delivering on digital services may be questionable. Overall, public trust is likely to be a key barrier to offering REVS to the country in the near future.

One of the significant benefits of implementing e-voting is supposedly a higher voter turnout. Voter turnout in the UK is considered low. In the 2019 general election, turnout was 67.3%, below the last 100 year average of 73%. [11] Therefore, many hope that introducing e-voting could encourage more people to vote. While we saw no substantial evidence that internet voting led to a higher turnout in Estonia, it did encourage more casual voters to vote regularly. Hence if we adopted REVS, perhaps it would halt our declining turnout. Interestingly, Estonia typically holds elections on Sundays, [45] whilst we conduct ours on a Thursday. Voting on a weekend means that voting in person was already somewhat convenient for much of their population, whilst our voters have to fit travelling to the polling station into their workday routine. So if we just changed the day of the week we conducted elections, we may see an increase in turn out. Although

one can argue that this change would also threaten the rituals and thus the everyday security people have with our established election procedure.

The government must also consider usability when designing an e-voting system. Failure to do so could marginalise communities within the population. We turn to the implementation of Universal Credit as an example of usability failure. Many disabled people claimed they could not navigate the complex system or complete the necessary forms if they were unwell. [56] Furthermore, nearly half a million people had to gain assistance from family and friends, the Jobcentre or a charity to apply. [57] Therefore, when applying this to e-voting, the government must consider how to make the system usable by all members of society, alongside what support they will offer those who require assistance.

Our last concern is that to break an electronic election, an attacker does not need to hack the system; they just need to cast enough doubt on the result. Disinformation campaigns on social media have emerged as a threat to society in the last few years, and the 2020 US presidential elections demonstrated it's ability to create doubt around the voting procedure. The rise in people opting to vote remotely using the postal vote was a sensible response to the pandemic. However, although there is consensus that voter fraud is rare and unlikely to swing an election, tens of millions of Americans believed the opposite. [58] A Harvard Kennedy School study found that around 65% of Trump voters believed that Trump was the actual winner of the 2020 election. [59] Therefore, if we introduced REVS in our general elections, it is likely that disinformation campaigns may lead to widespread acceptance that they are not to be trusted. Moreover, it is not just false beliefs spread by politicians and individuals that we need to be concerned about; Russian interference in the 2016 US presidential election and the Brexit referendum [60] demonstrates the risk to democracy, and the capabilities of foreign state actors. Perhaps we need to combat the rise of social media disinformation and interference from foreign states before we take our elections online. Failure to do so will create the potential for doubt to foster, and once conspiracies questioning the security of e-voting begin circulating online, it would be hard to regain trust from these individuals.

## 6 Conclusion

It has now been 16 years since Estonia first used REVS for an election, yet why hasn't the UK made any steps towards adopting e-voting? This paper has shown that electronic voting presents a significant challenge and requires research from various disciplines. We have highlighted the hurdles the UK would face in implementing a REVS, focusing on usability, trust, and the everyday.

Firstly, we have seen that the usability of a system can affect peoples intentions to vote. Voting systems worldwide are still challenging to use by disabled people or non-native language speakers, showing that usability still falls short despite equality efforts such as the Help America Vote Act. Furthermore, the digital divide is still a prominent issue in the UK that needs addressing; we need to be careful to ensure the system does not benefit the younger, highly educated members of society but is usable by the nation. Additionally, without a national ID infrastructure like that of Estonia, verification of voters becomes tough.

Next, obtaining public trust in a voting system is an onerous task. Not only does the system itself need to be trustworthy, but the public need to trust that it is. Additionally, factors beyond the system's security will affect perceived trust, such as the government, reputation, and friends and families opinions. Before the UK wishes to trial REVS, it must gain higher trust from the public before doing so, or else they may face threats from disinformation campaigns to cast doubt around the result.

Lastly, changing how we vote may threaten individuals everyday security since the process would not feel the same and challenges us to change the rhythm on which we vote. Although we argue that voting itself, whilst a long tradition, is incompatible with modern-day practices, perhaps moving it online enables more people to vote. While the lack of increase in voter turnout in Estonia indicates that those who wish to vote already will. Therefore, we need to do more to understand why people vote and work with non-voters to identify the reasons and potential barriers to choosing not to partake.

To conclude, voting is not a privilege but a fundamental right for all citizens; ergo, any voting system needs to be usable and accepted by the whole population. While implementing REVS is a cumbersome task, it is not impossible. Will e-voting become commonplace in the UK? Only time will tell, but what is important to conclude is that remote electronic voting is more than a technical challenge.

## References


[1] G. Qadah and R. Taha, "Electronic voting systems: Requirements, design, and implementation," *Computer Standards Interfaces*, vol. 29, pp. 376–386, Mar. 2007.

[2] L. Langer, H. Jonker, and W. Pieters, "Anonymity and verifiability in voting: Understanding (un)linkability," Sept. 2018.

[3] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of e-voting: the past, present and future," *Annals of Telecommunications*, vol. 71, June 2016.

[4] H. Buchstein, "Democracy's secret: Carl schmitt and the german critique of secret voting," *Redescriptions: Political Thought, Conceptual History and Feminist Theory*, vol. 6, pp. 107–125, Jan. 2002.

[5] J. Palas Nogueira and F. de Sá-Soares, "Trust in e-voting systems: A case study," in *Knowledge and Technologies in Innovative Information Systems* (H. Rahman, A. Mesquita, I. Ramos, and B. Pernici, eds.), (Berlin, Heidelberg), pp. 51–66, Springer Berlin Heidelberg, 2012.

[6] K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, "A review of contemporary e-voting : Requirements , technology , systems and usability," 2017.

[7] R. E. Rosacker and K. Rosacker, "A call for collaborative academic and practitioner efforts to address remote-access voting methods," *Transforming government*, vol. 6, no. 3, pp. 230–238, 2012.

[8] "Representation of the people act 1983. (c.2)." Available at `https://www.legislation.gov.uk/ukpga/1983/2/schedule/1` [Accessed: March 9th, 2021].

[9] K. Fuglerud and T. Halbach, "An evaluation of web-based voting usability and accessibility," *Universal Access in the Information Society*, vol. 11, Nov. 2011.

[10] M. Musiał-Karg, "Electronic voting as an additional method of participating in elections. opinions of poles," in *Electronic Voting* (R. Krimmer, M. Volkamer, J. Barrat, J. Benaloh, N. Goodman, P. Y. A. Ryan, and V. Teague, eds.), (Cham), pp. 218–232, Springer International Publishing, 2017.

[11] L. Audickas, R. Cracknell, and P. Loft, "Uk election statistics: 1918-2019 - a century of elections," Briefing Paper CBP7529, House of Commons Library, Feb. 2020. Available at `https://researchbriefings.files.parliament.uk/documents/CBP-7529/CBP-7529.pdf` [Accessed: March 3rd, 2021].

[12] K. Sál, "Remote internet voting and increase of voter turnout: Happy coincidence or fact? the case of estonia," *Masaryk University journal of law and technology*, vol. 9, no. 2, 2015.

[13] Y. Yao and L. Murphy, "Remote electronic voting systems: an exploration of voters' perceptions and intention to use," *European journal of information systems*, vol. 16, no. 2, pp. 106–120, 2007.

[14] N. Boulus-Rødje, "Mapping the literature: socio-cultural, organizational and technological dimensions of e-voting technologies," *n R. Krimmer R. Grimm (Eds.), Electronic Voting 2012 (EVOTE2012). Proceedings of the 6th International Conference EVOTE2012, Lecture notes in Informatics. Gesellschaft fu'r Informatik, Bonn.*, Jan. 2012.

[15] P. Kortum and M. D. Byrne, "The importance of psychological science in a voter's ability to cast a vote," *Current directions in psychological science : a journal of the American Psychological Society*, vol. 25, no. 6, pp. 467–473, 2016.

[16] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi, "Electronic voting system usability issues," in *CHI '03 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Apr. 2003.

[17] F. Conrad, B. Bederson, B. Lewis, E. Peytcheva, M. Traugott, M. Hanmer, P. Herrnson, and R. Niemi, "Electronic voting eliminates hanging chads but introduces new usability challenges," *Int. J. Hum.-Comput. Stud.*, vol. 67, pp. 111–124, Jan. 2009.

[18] "Ergonomics of human-system interaction — part 11: Usability: Definitions and concepts," standard, International Organization for Standardization, Mar. 2018.

[19] S. Laskowski, M. Autry, J. Cugini, W. Killam, and J. Yen, "Improving the usability and accessibility of voting systems and products," Special Publication 500-256, NIST, May 2004. Available at `https://www.nist.gov/system/files/documents/itl/vote/FinalHumanFactorsReport5-04.pdf` [Accessed: March 3rd, 2021].

[20] K. Marky, M.-L. Zollinger, M. Funk, P. Ryan, and M. Mühlhäuser, *How to Assess the Usability Metrics of E-Voting Schemes*, pp. 257–271. Mar. 2020.

[21] S. Everett, M. Byrne, and K. Greene, "Measuring the usability of paper ballots: Efficiency, effectiveness, and satisfaction," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 50, Oct. 2006.

[22] J. Budurushi, M. Volkamer, O. Kulyk, and S. Neumann, "Nothing comes for free: How much usability can you sacrifice for security?," *IEEE Security Privacy Special Issue on Electronic Voting*, vol. 15, Jan. 2017.

[23] K. Marky, O. Kulyk, K. Renaud, and M. Volkamer, "What did i really vote for? on the usability of verifiable e-voting schemes," pp. 1–13, Apr. 2018.

[24] B. A. Campbell, C. C. Tossell, M. D. Byrne, and P. Kortum, "Toward more usable electronic voting: Testing the usability of a smartphone voting system," *Human factors*, vol. 56, no. 5, pp. 973–985, 2014.

[25] P. Serafino, "Exploring the uk's digital divide," article, Office for National Statistics, Mar. 2019. Available at `https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04#introduction` [Accessed: March 3rd, 2021].

[26] P. van den Besselaar, A. Oostveen, F. D. Cindio, and D. Ferrazzi, "Experiments with e-voting technology: Experiences and lessons," 2003.

[27] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, and M. Traugott, "The importance of usability testing of voting systems," in *2006 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 06)*, (Vancouver, B.C.), USENIX Association, Aug. 2006.

[28] M. Germann, "Making votes count with internet voting," *Political Behavior*, Mar. 2020.

[29] A. Ongsarte, Y. Jiang, and K. McMullen, "Assessment of electronic write-in voting interfaces for persons with visual impairments," pp. 418–423, Aug. 2015.

[30] J. Ismirle, I. O'Bara, J. E. Jackson, and S. J. Swierenga, "Touchscreen voting interface design for persons with dexterity impairments: Insights from usability evaluation of mobile voting prototype," in *HCI in Business, Government, and Organizations: Information Systems* (F. F.-H. Nah and C.-H. Tan, eds.), (Cham), pp. 159–170, Springer International Publishing, 2016.

[31] L. Schur, M. Ameri, and M. Adya, "Disability, voter turnout, and polling place accessibility," *Social Science Quarterly*, vol. 98, no. 5, pp. 1374–1390, 2017.

[32] J. Mohen and J. Glidden, "The case for internet voting," *Commun. ACM*, vol. 44, p. 72–ff., Jan. 2001.

[33] A.-M. Oostveen and P. Van den Besselaar, "Security as belief user's perceptions on the security of electronic voting systems," Jan. 2004.

[34] W. Pieters, "Acceptance of voting technology: Between confidence and trust," pp. 283–297, May 2006.

[35] M. Turilli, A. Vaccaro, and M. Taddeo, "The case of online trust," *Knowledge, Technology Policy*, vol. 23, pp. 333–345, Dec. 2010.

[36] E. Fragnière, S. Grèzes, and R. Ramseyer, *How do the Swiss Perceive Electronic Voting? Social Insights from an Exploratory Qualitative Research*, pp. 100–115. Sept. 2019.

[37] A. Crawford and S. Hutchinson, "Mapping the contours of 'everyday security': Time, space and emotion," *British journal of criminology*, vol. 56, no. 6, pp. 1184–1202, 2016.

[38] L. Coles-Kemp and R. Rydhof Hansen, "Walking the line: The everyday security ties that bind," in *Human Aspects of Information Security, Privacy and Trust*, vol. 10292 of *Lecture Notes in Computer Science*, pp. 464–480, Springer, 2017.

[39] M. Solvak and K. Vassil, "Could internet voting halt declining electoral turnout? new evidence that e-voting is habit forming," *Policy and internet*, vol. 10, no. 1, pp. 4–21, 2018.

[40] M. Toots, T. Kalvet, and R. Krimmer, "Success in evoting – success in edemocracy? the estonian paradox," in *Electronic Participation*, Lecture Notes in Computer Science, (Cham), pp. 55–66, Springer International Publishing, 2016.

[41] Valimised, "Statistics about internet voting in estonia." `https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia` [Accessed March 9th, 2021].

[42] E. Maaten, "Towards remote e-voting: Estonian case.," pp. 83–100, Jan. 2004.

[43] G. Schryen and E. Rich, "Security in large-scale internet elections: A retrospective analysis of elections in estonia, the netherlands, and switzerland," *IEEE transactions on information forensics and security*, vol. 4, no. 4, pp. 729–744, 2009.

[44] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security analysis of the estonian internet voting system," (New York, NY, USA), Association for Computing Machinery, 2014.

[45] R. M. Alvarez, T. E. Hall, and A. H. Trechsel, "Internet voting in comparative perspective: The case of estonia," *PS, political science politics*, vol. 42, no. 3, pp. 497–505, 2009.

[46] M. Kalkun and T. Kalvet, "Digital divide in estonia and how to bridge it," *Tallinn: Emor and PRAXIS Center for Policy Studies*, Jan. 2004.

[47] "Indivduals using the internet (% of population)." `https://data.worldbank.org/indicator/IT.NET.USER.ZS?year_high_desc=true`. Accessed: March 7th, 2021.

[48] P. Teffer, "Build trust before you introduce e-voting, says estonian president)." `https://euobserver.com/digital/138394`, June 2017. Accessed: March 10th, 2021.

[49] F. Stephany, "It's not only size that matters: determinants of estonias e- governance success," *Electronic Government*, vol. 16, no. 3, pp. 304–313, 2020.

[50] C. Avgerou, "Explaining trust in it-mediated elections: A case study of e-voting in brazil," *Journal of the Association for Information Systems*, vol. 14, no. 8, pp. 420–451, 2013.

[51] J. Nurse, I. Agrafiotis, A. Erola, M. Bada, T. Roberts, M. Williams, M. Goldsmith, and S. Creese, "An independent assessment of the procedural components of the estonian internet voting system," *SSRN Electronic Journal*, Jan. 2016.

[52] K. M. Rosacker and R. E. Rosacker, "Voting is a right: a decade of societal, technological and experiential progress towards the goal of remote-access voting," *Transforming government*, vol. 14, no. 5, pp. 701–712, 2020.

[53] D. Clarke, F. Hao, and B. Randell, "Analysis of issues and challenges of e-voting in the uk," pp. 126–135, Apr. 2012.

[54] "Is boris johnson trustworthy?." `https://yougov.co.uk/topics/politics/trackers/is-boris-johnson-trustworthy`. Accessed: March 11th, 2021.

[55] A.-M. Oostveen, "Gauld, r., goldfinch, s. (2006). dangerous enthusiasms: E-government, computer failure and information system development. dunedin, new zealand: Otago university press 160 pp.," *Social Science Computer Review - SOC SCI COMPUT REV*, vol. 26, pp. 257–259, 12 2007.

[56] C. Pearson, "Independent living and the failure of governments," *Routledge Companion to Disability Studies*, 2019.

[57] L. Coles-Kemp, D. Ashenden, A. Morris, and J. Yuille, "Digital welfare: designing for more nuanced forms of access," *Policy Design and Practice*, pp. 1–12, May 2020.

[58] Y. Benkler, C. Tilton, B. Etling, H. Roberts, J. Clark, R. Faris, J. Kaiser, and C. Schmitt, "Mail-in voter fraud: Anatomy of a disinformation campaign," *Available at SSRN*, 2020.

[59] G. Pennycook and D. G. Rand, "Research note: Examining false beliefs about voter fraud in the wake of the 2020 presidential election.," *Harvard Kennedy School (HKS) Misinformation Review.*, 2021.

[60] E. McGaughey, "Could brexit be void?," *King's Law Journal*, vol. 29, no. 3, pp. 331–343, 2018.