Design Alternatives to the Ballot Box Voting System
Anthony Crabbe

Introduction
Western democracy has always been an idea dependent on the design of physical systems that enable citizen participation in decision-making. Athenian citizens of the fifth century BCE helped implement Kleisthenes’s new system of governance by dropping tokens indicating either “for” or “against” into amphorae, which could be emptied and whose contents counted publicly to ascertain the majority’s decision. That original design still persists in most democracies today, where the most noticeable physical difference is that paper ballots and lockable boxes replace tokens and jars. A more significant system difference is that public balloting today is used primarily for the election of governmental representatives and the political parties to which they belong. This party political (or “representative”) system of democracy is often called the “Westminster” system, after the customs and practices of British parliaments of the seventeenth and eighteenth centuries. In marked contrast, the original Athenian democracy was a “direct” one, in which all major policies were decided by a popular ballot, rather than a restricted ballot within the boule (i.e., the standing council of 500 regional representatives, and the forerunner of present-day congresses). Moreover, members of the boule and the legislature were not voted into office. They were citizens selected by lot, using an ingeniously designed lottery device, carved from stone and called a kleroterion.

Thus, any notion that the Westminster system had revived the principles and values of Athenian democracy was a fanciful conceit of British parliamentarians, who had only really created a system for deciding which of their various factions could take a fixed period turn at governing the nation. As British Lord Chancellor Quintin Hogg suggested in 1976, their Westminster system might better be described as an “elective dictatorship,” in which citizens play no role other than to decide which individual should represent their locality inside an institution that Dickens characterized as “the best club in London.”

3 Quintin Hogg, Elective Dictatorship, Richard Dimbleby Lecture, October 14, 1976, BBC TV.

doi:10.1162/DESI_a_00222
organize themselves to conduct such business, what hours they work, what pay and expenses they receive, who may lobby them, and so forth. Republican democracies have tried to balance the powers of such self-validating representative assemblies through the office of a president, elected in place of the hereditary constitutional monarch of the Westminster prototype.

The different uses of ballot boxes in ancient and modern eras then indicate key issues to be addressed by anyone interested in designing a more contemporary political balloting system. Modern information and communication technologies (ICT) naturally suggest far more effective means of balloting, characterized as “e-voting,” as well as greater opportunities for canvassing and expressing public opinion, characterized as “e-democracy.” Since the late 1990s, ICT voting platforms have enabled audiences to cast votes for game show contestants using touch-tone telephones, and many large organizations elect their senior officers using Internet voting platforms. In the past decade, many governments have conducted trials of Internet voting, as well as various trials of telephone voting at a regional level in countries including Canada, The Netherlands, and the United States. Despite all these trials, at the time of writing, Estonia appears to be the only nation that has an Internet voting system for national elections.

This slow progress appears surprising in light of continuing public demonstrations around the world against election results obtained by paper balloting, and indeed, some polling machines, as in the “hanging chad” furor following the disputed results of the U.S. 2000 presidential election. This lack of design success raises the question of what the obstacles to devising a successful system are. Regardless of the design category in which we might choose to place e-voting systems—whether product, interface, or service design—the design of all physical voting systems clearly involves factors both human and technical. Since the political nature of any democratic voting system invokes peoples’ sense of their “rights,” voting systems naturally raise competing notions of rights, both between different groups of citizens and between citizens and politicians. Such competition makes e-voting a highly unusual example of product or service design. To demonstrate how unusual a “service” political e-voting is, this article examines a case study of a proposed telephone voting system design, which seeks to overcome the security problems inherent in the physical form of Internet systems by using encryption methods now familiar in both telephone and Internet banking. As the case study shows, the human factors that confronted this particular design proposal presented far more significant obstacles to its successful implementation than any of the technical issues encountered.

The Differences Between e-Voting Platforms

“E-voting” is a vague term used to describe fundamentally different ICT platforms. Such platforms include: 1) Internet systems, 2) polling booth machines, and 3) telephone voting systems. Further confusion arises from the conflation of the terms e-voting and “e-democracy.” The former is a neutral description of the kind of activity enabled by the three ICT systems listed, whereas e-democracy is a theorized consequence of people’s use of some form of ICT platform to disseminate their views, even though such a platform (e.g., a website or a Twitter thread) might not offer any voting functions at all.

Computer-connected polling booth machines have proven to be the most successful ICT voting platforms, and are now used in political elections in a number of major democracies, including India, Brazil, France, and the United States. Unlike earlier recording machines, of the sort used in the U.S. 2000 presidential election, the telephonically connected ones transmit voters’ choices to a central computer system, which obviates the labor of collating the results of many stand-alone machines and gives a final result within hours of the closing of the polls.

Internet voting systems aim to go one step further by enabling electors to vote remotely from a polling station, using the web on any personal computer or web-enabled mobile phone. The labor-saving potential of this platform, as well as its connectivity to e-democracy websites makes Internet voting the most widely discussed ICT platform. Unfortunately, the security issues involved also make it the most controversial one proposed.

Telephone voting, as originally conceived by those such as Buckminster Fuller, involved employing switchboard operators to record the outcome of telephone conversations with callers. But since the digitalization of telecommunication technologies in the 1990s, telephone voting has become an ICT system, where a central computer can record the tones generated when callers press the phone’s number pad. The convergence of computer and mobile phone technologies also enables other possibilities, such as the use of short message service (SMS) capabilities, voice activated relays, or a web application. In terms of remote voting then, the telephone has the following clear advantages over Internet voting systems:

- Globally, access to and ownership of telephones is far higher than that of computers. The personal ownership of mobile telephones alone is estimated to be 60%, while only 20% have access to PCs, including corporately owned ones.
- Successfully using the basic functions of a telephone requires far less knowledge than using a computer; phone “literacy” is far higher than computer literacy.

---

Telephone functions cannot be over-taken by hackers in the same way as those can be of a computer.

Telephones can only communicate with a computer system by relaying sounds rather than data; thus, phone signals cannot be used to modify the computer software.

The costs of a telephone voting system can easily be recovered by using standard phone call charging, but they cannot be easily recovered from a web-based system without use of an e-commerce application. Cost recovery from the labor-intensive polling machine system is even more difficult and, in practical terms, could only be achieved through public taxation.

These advantages appeared even more evident in the late 1990s than at present, which makes astonishing the fact that Internet voting has attracted so much more public and research interest than telephone voting. An examination of the reasons for this comparative level of interest in the two remote voting platforms is beyond the scope of this article, but the effects warrant a brief commentary. The current consensus of expert opinion on Internet political voting is hostile. This hostility has naturally frightened off many e-voting initiatives by politicians, including the one to give U.S. forces personnel serving in war zones the opportunity to vote remotely. A PBS News Hour report of this initiative shows computer researchers from the University of Michigan jubilantly “high-fiving” after they responded to an open challenge from West Virginia politicians to hack into their trial web-voting site, and succeeded in causing it to malfunction in many ridiculous ways. Missing from the report was the fact that it took the team 36 hours to hack into the site, when most election polls do not open for longer than 18 hours. However, the ridicule successfully illustrates the security issues that have brought about the hostile expert consensus and have led to reversals by former advocates of Internet voting (e.g., Jason Kitcat), who now advocate against e-voting initiatives.

Regrettably, the new negativity about Internet voting stands to prejudice all endeavors to develop ICT-enabled political voting, especially when the generic term “e-voting” is applied to every such design proposal. An advocate of telephone voting systems might tell e-voting skeptics that their reservations about the Internet as a suitable e-voting platform simply confirm the advantages of the telephone as the most suitable platform, and therefore, most of their e-voting security fears are misplaced. In order to better understand the kind of security issues that confront the designer of any remote ICT political voting system, it is next necessary to outline the generic technical design requirements.

---


Design Criteria for a Remote ICT Political Voting System

In the early 2000s, before national governments started formulating their own standards for e-voting systems, ICT experts had started developing design criteria that still underpin most of the subsequent standards. For example, the U.S.-based Internet Policy Institute made the following list of criteria its members believed would be necessary to ensure both public and official confidence in any remote voting system:

- **Authentication**: Only authorized voters should be able to vote.
- **Uniqueness**: No voter should be able to vote more than once.
- **Accuracy**: Voting systems should record the votes correctly.
- **Integrity**: Votes should not be able to be modified without detection.
- **Verifiability**: Verifying that votes are correctly counted in the final tally should be possible.
- **Auditability**: Reliable and demonstrably authentic election records should be generated.
- **Reliability**: Systems should work robustly, even in the face of numerous failures.

To this early list of criteria drawn up for Internet voting, I suggest the following should be added to any comprehensive list of e-voting criteria:

- **Anonymity**: Voters must feel confident that their personal decision remains private.
- **Accessibility of hardware**: Hardware should be easily accessible to remote voters.
- **User intelligibility**: Voting options should be clear to voters.
- **Data traffic handling**: The system must be capable of handling high demand over a short period.
- **Data protection**: Database owners must comply with data protection laws.
- **Traceability**: Election officers may need to trace votes back to their originators (e.g., U.K. law).
- **Ownership**: Subcontractors should not end up owning any data collected by their systems.
- **Cost effectiveness**: Public election costs should be kept to the minimum possible.

This formidable list contains requirements that could each take a number of papers to fully discuss. I review most of these criteria here by reference to a case study, which is a telephone voting system on which I worked between 1999 and 2008. What might prove

---

particularly interesting about this project is the nature of the obstacles that finally halted the progress and enthusiasm of the people involved. Principal among these obstacles was the questionable dedication of Westminster officials to actually introduce any form of e-voting, as distinct from their commitment to arranging an on-going succession of public trials.

Case Study: A Telephone Voting System Using Partial Identifiers
One inspiration for this project was the emergence of television game shows in the late 1990s that used telephone voting to select winning contestants, either directly or by successively ostracizing the least popular contestants until a winner emerged. Political scientist Stephen Coleman was a sensitive observer of this phenomenon, recognizing in this apparent theatre of cruelty many parallels with the relationship between political representatives and their electorates. Aside from the obvious parallels between the ritual ostracisms of ancient Athens and the “voting off” of television contestants, these telephone votes cast on premium call lines generated immense additional revenues for both the game shows’ producers and their call handlers, thus demonstrating how telephone voting technology provided a novel way of recovering election costs and, thereby, addressing the final design criterion listed, cost effectiveness. The challenge then, was to redesign this commercially clever use of new developments in ICT to serve the more serious purpose of political voting.

Our project group started by thinking about how to address the criterion of “authentication,” which concerns the means by which a telephone voting system can distinguish legitimate from illegitimate electors. In many countries, every authorized elector has at least two personal identification numbers (PINs) allocated to him or her by the state, and in state databases, these PINs are linked to other information, such as name and address. In the United Kingdom, two such PINs are a nine-character social security number (six of them digits) and an eight digit voter identification number (VIN). The two databases on which these PINs are held also contain names and addresses, which should both be the same if the records are up to date. Data protection laws do not allow these two state agencies to share information, except in the case of a criminal prosecution; thus, the data they share in common—a name and address—do not belong to any database containing both these PINs.

This common factor of name and address then suggests a design solution: As illustrated in Figure 1, we create a third database by asking each state agency to supply a list of only, for example, the first six digits of all the eight- or nine-digit PINs they have allocated to registered citizens. Against each partial PIN, the owners supply the citizen’s postal code (but not their house number or street). This approach meets the criterion of “anonymity” because
the data used to create a list of authorized voters comprises only partial PINs and postal codes but not house numbers or personal names. The database owners can forward the data in the password format, “••••,” which cannot be read by any employee of the ballot organizer. The ballot organizer then has a third database that, even if they could read it, would not tell them anything more than the area in which an unnamed individual lives. Therefore, the argument can be made that the database owners are not breaching data protection legislation because they are not sharing information with the ballot organizer about any individual the organizer could possibly identify from its own database. The inclusion of postal codes further helps the organizers to address the criterion of “accuracy” by enabling them to sort their database by postal codes that relate to the appropriate electoral constituencies.

The organizer’s database of authenticated voters then comprises two partial PINs for each voter, each of which could belong to at least a hundred individuals, related to two instances of the same postal code. Wherever two such PINs both relate to the same one postal code, the certainty that the two PINs belong to one state-registered individual is extremely high. For example, in the U.K., the same residential postal code is typically shared between 15 and 30 households, or on average, between 40 individuals. 14 Approximately 45 million U.K. citizens are eligible to vote. 15 Therefore, the total number of possible individuals $i$, who could be identified by some combination of two six-digit PINs and one of 1.25 million residential U.K. postal codes can be expressed by the following equation:

$$i = (n1) (n2) (V/P)$$

Where $n$ = the total number of six-digit PIN permutations, $V$ = the size of the voting population, and $P$ = the number of individuals sharing one common postal code. Plugging in the U.K.’s authorized voting population, the value of $i$ is then:

$$i = (10^4) (10^4) (45 \times 10^6)/40 = 1.125 \times 10^{18}$$

Because only 45 million of the possible individuals in $i$ are the true authorized voting population $V$, the odds that any rogue caller who randomly enters two six-digit PINs and actually manages to enter two connected by a common postal code are:

$$Odds = (i: V) = (1.125 \times 10^{18}; 4.5 \times 10^6) = 2.5 \times 10^{12}: 1$$


To put these odds of 250 billion to 1 into perspective, every one of the 4 billion people on earth who own a mobile telephone would have to make 63 calls each, and enter two unique PINs each time, before one of them was successful in logging on as an authorized U.K. voter. (In the United States the same postal code can be shared by a number of households, ranging from 3,000 to 100,000.16) Therefore in the United States it would be necessary to use PINs with more characters in order to get the same level of certainty; thus, U.S. voters might be asked for, say, seven digits of a ten-digit PIN). This partial PIN solution then gives not only near certainty that the first criterion of “authentication” is met, but also the same level of confidence that the system can address the contradictory pull of the criterion for “traceability.” Given the odds, those who had keyed in two partial PINs sharing a common postal code would have difficulty denying that they were identifying themselves as a particular individual who could easily be named by fraud investigators who have legal access to both originating databases.

This contingency does reveal the need to set up the vote-recording computer to meet the “uniqueness” criterion, so that only one vote is accepted against any successfully registered caller. Furthermore, the software on the recording computer needs to be programmed to alert both the ballot organizer and the individual voter if more than one attempt is made to log on using that voter’s PINs. A problem already encountered in traditional paper balloting systems is that people enter the same polling station several times using the VINs of other household members they believe won’t be voting. This is one of the reasons why U.K. law demands traceability. Clearly, independent phone company records would prove useful in assisting identity theft investigations, particularly if public pay phones were barred from calling the voting line.

As illustrated by Figure 2, a telephone voting system is controlled by computers that are programmed to respond to sound signals relayed through the telephone exchange. Nobody outside of the control system can communicate with it directly by using

---

Design Issues: Volume 29, Number 3  Summer 2013

computer software, which eliminates the system’s vulnerability to hacking. Thus, the three primary security concerns are: (1) data theft by employees of the ballot organizer, (2) alteration of data when they are handed over to the electoral office, and (3) illicit recording of calls or messages by the various telephone carriers who connect the voter to the ballot organizer. The precautions against the first issue would be the same ones as those used to monitor employees of financial institutions, such as banks, while the precaution against the second would be for the ballot organizer to make back-up copies of the main database, which can be warehoused with a trusted third party that has nothing to gain from the results of the particular ballot. For the third concern, telephone carriers in most democracies already operate within a legal framework that makes illicit call recording a self-damaging exercise.\(^{17}\)

The actual voting is then a three-part process comprising registration, voting, and verification, which is a limited period during which the caller can verify that the choices the ballot organizer has recorded against an anonymous identity are accurate, as is illustrated schematically in Figure 3.

Notice that in this embodiment of a telephone voting system, the caller is guided and directed by a menu of voice instructions that require responses on the touch-tone number pad of a telephone. This approach is preferable to using SMS because the sound signals sent cannot legally be recorded or stored by telephone carriers. Individual SMS records can be hacked both from service providers and personal phones, as evidenced by the open sale of invasive software for that purpose.\(^{18}\) Furthermore, the voice-activated response interfaces used in a lot of present telephone voting software obviate even the need for number pads, and may help better address the criterion of “user intelligibility.” Another design

---

The design of this system then appears to address the crucial security issues in the list of design criteria, which the opponents of e-voting say cannot be addressed by Internet voting systems. The only technical obstacles the telephone system appears to raise are those concerning traffic handling and data sharing by the various database owners. Our original design was made with British Telecom’s (BT’s) Meridian telephone voting system in mind, which had been used for various television shows. Its present successor, Agilemedia, is set up with a call handling center consisting of 28,000 lines. One national application of Agilemedia was severely tested by the 2010 Pop Idol contest that generated 80 million call attempts in one day (three quarters of all the normal daily U.K. call traffic). Accordingly, the traffic generated by a national election would require the capital investment needed to set up a number of such call-handling centers.

Combining the data from a number of state agencies onto an electoral one presents more complex issues of ownership and rights that would require state intervention at the most senior level to resolve them. Not least of the problems in the U.K., and in some
other countries as well, is that the electoral offices that compile electoral registers and issue VINs are actually quasi-autonomous ones that operate out of local government offices. Therefore, our preliminary investigations revealed that our design proposal would depend on the goodwill and cooperation of state agencies and government at both national and local levels. This dependence proved to be a major obstacle to our endeavors to be included in U.K. national trials of e-voting systems in 2003 and 2007.

**Human Factors as Obstacles to Political Telephone Voting**

Having initially approached BT to help us develop our system under their *Brightstar* initiative, we were dismayed to discover that the long-promised U.K. e-voting trials promised by the Labour government’s Office of the Deputy Prime Minister (ODPM) were to be run under new protocols clearly written to encourage applications from an established group of government sub-contractors for new ICT developments, such as computerized police and healthcare systems. The terms of the protocols also meant that the suppliers would need to design a satisfactory “front end” to their systems (i.e., design the user interface), which would involve further design criteria concerning, for example, the clarity of information, ease of use, and fail-safes against user error. However, at that time, many research groups, including ours, had been focused on the underlying system architecture, in the expectation that the client would be collaborating in the design of the user interface they wanted.

The publication of the ODPM’s protocols then made BT, along with many small research groups, withdraw from what was now evidently a tendering process for contractors to supply ready-made systems for trials in local elections.21 This development undercut our earlier understanding that the ODPM would be taking a proactive role in bringing together a number of researchers to collaborate in identifying the most satisfactory architectures for further development. Such an approach would be the normal expectation if an organization were seeking to develop a sensitive service. For example, it is unimaginable that any bank developing online banking would not want to work closely with the designers in developing the front end of any particular ICT architecture the designers had proposed. With the strategy now appearing to be one of government procurement, the only telephone voting platform that proved ready for U.K. trials in 2007 was the Opt2Vote platform, developed by the established European information management specialists Idox plc.22 The system was based on an SMS messaging system that tested quite satisfactorily in 2007.23 But unlike the various postal voting systems Idox have developed, Opt2Vote has not yet been adopted for general use in U.K. elections. (Ironically, the partial PIN system we patented is now widely used...

---

used by banks, such as Barclays, to authenticate remote users of their Internet and telephone banking systems, where excellent security is obviously a prerequisite.

The fact that major corporations, as well as small research groups, have struggled to establish telephone voting systems through schemes organized within the Palace of Westminster naturally draws attention to the features of e-voting that do not recommend themselves to the officers of representative democracies. E-democracy, with which e-voting is commonly conflated, is widely seen to be a first step toward changing representative into direct democracy. Writing at the dawn of the e-democracy movement in 1993, Brian Needham pointed out that any development toward direct democracy would rob political parties of most of their “functions” and “grandeur.”

Establishing voting systems that could be easily used by an electorate has then always been seen as a natural first step toward direct democracy, as evidenced in Buckminster Fuller’s 1963 proposal of telephone voting, long before the “e” label was envisioned:

Devise a mechanical means for nation-wide voting daily and secretly by each adult citizen of Uncle Sam’s family: Then - I assure you - will Democracy “be saved,” indeed exist, for the first time in history…25

Given the potential of such a system to replace representative democracy with what has sometimes been characterized as a “mobocracy,” largely informed by the popular press, the reluctance of both political experts and ordinary citizens to endorse any movement toward direct democracy might be understandable. With voters in the younger generation far more accustomed to ICT playing a major role in their decision-making, a growing level of public confidence could be a reasonable expectation. If so, then the eventual introduction of an ICT voting system would likely lead to greatly increased public pressure for a transition from the occasional paper ballot to more frequent telecommunication elections.

In that event, the voting system would likely lead to challenges of the unpalatable features of a Westminster system. Anyone who believes that an executive assembly of elected representatives should be accountable to their electorate for the ways in which they conduct their business might then believe that more direct electoral powers would allow for significant improvements in a Westminster system. What many present representative democracies appear to lack is “accountable” democracy, which might help to explain the growing voter apathy in those democracies that do not compel their citizens to vote in general elections.26

Imagine then, the revolutionary effect of any series of telephone ballots in which the electorate petitions the state through motions that offer the following kinds of voting choices:

25 Buckminster Fuller, No More Second Hand God, 10.
I call upon parliament to select five members by lot who will give the electorate an opportunity every four years to decide which type of voting system they wish to use in elections. Yes/No

I call upon members of parliament to vote privately on all policy decisions and ban the practice of party whipping. Yes/No

How could any majority party government claim the same mandate to govern in the traditional Westminster manner if a majority of the same electorate that had voted every member of the representative assembly into office were to make such demands? As Needham argues, Westminster system representatives have every reason to fear an easily accessible and manageable popular voting system. To claim that such fears directed the ODPM’s unanticipated procurement approach in the 2000s would be too speculative. However, its unwillingness to actually lead in the creation of an effective e-voting system certainly heightened our suspicions that the ODPM was playing a well-established political game by appearing to investigate a given reform just long enough to take the wind out of the reforming movement’s sails. Regardless of whether this suspicion describes the ODPM’s strategy, the effect of Westminster’s continuing ten-year prevarication over e-voting has been to push the e-voting agenda far into the background of current U.K. politics. The immediate effect on our design and development plans was to prevent our work on the systems architecture from ever progressing to the next stage of the user interface testing or to other co-design strategies familiar to designers of ICT services.27

Conclusion

By a deft stroke, Westminster has now promoted e-democracy above e-voting by setting up an e-petition site, open to all members of the public to both propose and vote on various initiatives of their own devising.28 Any cursory examination of the list of the petitions on offer would reveal the majority to be nationally insignificant, and often rather eccentric. Not surprisingly, most have failed to collect even the 100,000 votes required to guarantee a parliamentary debate. Furthermore, we might reasonably suspect that the same group of people has voted for many of the petitions raised, and the authentication procedure for adding a signature is very weak in terms of the design criteria previously discussed. Hence, the argument that the principal obstacles to e-voting are technical ones appears unconvincing. On the contrary, e-voting appears to be a design proposal that cannot be realized simply on the basis of technical demonstration. Its potential behavioral effect could make the much-vaunted benefits of ICT-enabled social sites and feeds appear relatively trivial. If citizens were able to evidence their solidarity for some cause through a verifiable telephone poll,

28 http://epetitions.direct.gov.uk (accessed March 27, 2012.)
rather than through large gatherings organized through ICT social networks, as seen during the “Arab Spring” of 2011, then not only would the level of physical risk be reduced, but the certainty about the level of popular support would be far greater.

In other words, the more simple, immediate, and effective is the design of an e-voting system, the greater is the threat it poses of transferring actual decision-making powers from politicians to citizens. Thus, the successful implementation of any e-voting design in a large nation almost certainly requires citizens’ sustained advocacy for it. Yet citizen groups generally lack the same level of organization and authority of their politicians. Within this body of citizens, some will demand more direct powers than others; and outside this body, others will fear that the implementation of e-voting could lead to an even less desirable form of governance than their existing one. These key factors make political e-voting systems unlike other types of service design. The political system must provide a single, universal service to its users, but not all users share the same view about what the service should be providing. In turn, the governmental “service provider” has a strong motivation to restrict the potential of the service to serve as a vehicle for any challenge to its current authority and privileges. Thus, as with environmentally responsible design proposals, political e-voting appears to be an idea that cannot be implemented just because an effective design proposal has been offered. Any such proposal that is not supported by vigorous popular advocacy, which is likely to involve confronting the current service providers (politicians), appears unlikely to be realized in the near future.