Ethics of e-voting
An essay on requirements and values in Internet elections

W. Pieters
Institute for computing
and information sciences
Radboud University Nijmegen
P.O. Box 9010
6500 GL Nijmegen
The Netherlands
tel. +31 24 365 25 99
fax +31 24 365 31 37
wolterp@cs.ru.nl

M.J. Becker
Centre for ethics

Radboud University Nijmegen
P.O. Box 9103
6500 HD Nijmegen
The Netherlands
tel. +31 24 361 62 26
fax +31 24 361 55 64
mbecker@phil.ru.nl

Abstract

In this paper, we investigate ethical issues involved in the development and implementation of Internet voting technology. From a phenomenological perspective, we describe how voting via the Internet mediates the relation between people and democracy. In this relation, trust plays a major role. The dynamics of trust in the relation between people and their world forms the basis for our analysis of the ethical issues involved. First, we consider established principles of voting, confirming the identity of our democracy, which function as expectations in current experiments with online voting in the Netherlands. We investigate whether and how Internet voting can meet these expectations and thereby earn trust, based on the experiments in the Netherlands. We identify major challenges, and provide a basis for ethical and political discussion on these issues, especially the changed relation between public and private. If we decide that we want to vote via the Internet, more practical matters come into play in the implementation of the technology. The choices involved here are discussed in relation to the mediating role of concrete voting technologies in the relation between citizen and state.

Keywords: Internet voting, ethics, democracy, voting, security, trust, mediation

INTRODUCTION

It is often heard that democracy faces a crisis. Whether democracy is really in a crisis is hard to tell. People are eager to use the term "crisis" when something suddenly receives a lot of attention, but research often indicates that such hypes have existed throughout history[1]. However, the atmosphere

[1] Already in 1927, the public was said to be in an eclipse (Dewey, 1991).

of victory and triumph that surrounded western democracy after the breakdown of the wall has, more and more, been accompanied by the recognition that current-day democracy is not an ideal solution either. In the Netherlands, there is even said to be a feeling of "onbehagen"[2]. Many complain that the rise and murder of Pim Fortuyn have not really changed anything in the political system, except the fact that the parliament building has changed into some kind of fortress. The emotions in the public sphere that Fortuyn appealed to have not found a stable way to express themselves.

The increasing indifference or even antipathy towards politics, combined with the emergence of populism, may indeed be a serious problem. In a time of growing indifference towards politics, governments are eager to adopt any measures that may provide citizens with the ability to express their views in the most convenient way. Anything will do to involve the public. Politicians in the Netherlands discuss new administrative arrangements: a chosen mayor and more focus on regional candidates in parliament elections. Also "e-democracy" is mentioned: democracy via the Internet. We may distinguish between at least three possibilities for e-democracy: representative (elections), consultative (referenda) and participatory (discussion)[3]. People may choose their representatives via the Internet, people may vote on concrete decisions, or people may be involved in online discussion and deliberation.

Of all the e-democracy initiatives, especially Internet voting[4] is getting more and more attention. Governments and authorities are interested in its possibilities and stimulate experiments[5]. Governments are eager to say that they want to stimulate online voting because they expect it to increase turnout. Also the people themselves move the train (demand-pull). In the Netherlands, 62 % of the people with access to the Internet would prefer to vote online[6]. Where people do their banking online, buy tickets and books online, why do they have to move to a polling station to cast their vote? It is not so clear, however, which reasons for introducing Internet voting can withstand criticism. There is no proof for increased turnout. Experiments suggest no change, or even a decrease[7]. Neither do voters *expect* it to increase turnout substantially[8]. And does a comparison of voting to banking and buying tickets do justice to the particular characteristics of voting? Is it really only a change of means in collecting votes?

There is always a temptation to consider technology as morally neutral. In this case: votes are votes; the technology for transmitting the votes to central registration office does not have any influence on the voting process. However, it has been shown in other cases that technology may profoundly change people's life and our society. As with the introduction of all new technical systems, it is necessary to make explicit the moral questions at stake. In this paper, we will

[2] discomfort, uneasiness, malaise

[3] The second and third item in this list may be considered as two different means of achieving deliberative democracy. Referenda then correspond to what is called Direct Voting Democracy, and participation in discussion corresponds to Iterative Deliberative Democracy (Alvarez & Hall, 2004).

[4] In this paper, we will use the terms "Internet voting" and "online voting" synonymously, in the sense of remote Internet voting (from any computer connected to the Internet). We do not discuss other forms of Internet voting that use access restrictions (Alvarez & Hall, 2004: 4). In the title, we mean e-voting as in e-commerce, i.e. electronic *and* remote. E-voting is also used for voting machines by some people, and that is why we avoid the term in the discussions.

[5] Some steps have already been taken. In the Netherlands, more and more people determine their vote in an election completely or partly based on the outcome of the "stemwijzer", an online vote consultant (De digitale revolutie: onderzoeken februari 2003, http://www.dedigitalerevolutie.nl/onderzoek/onderzoek.htm, consulted February 24, 2005). This is a completely new means of choosing (or confirming) what to vote. From this perspective, it can be proposed to add a button to cast the vote immediately.

[6] Burger@overheid publiekspanel: stemmen via internet, http://www.burger.overheid.nl/publiekspanel/?id=253, consulted February 24, 2005

[7] See e.g. Oostveen & Van den Besselaar (2004). Also, the first elections with the RIES system, which will be discussed later, showed decreased turnout.

[8] Oostveen & Van den Besselaar (2004)

investigate the issue of Internet voting from a phenomenological inspiration: we focus on the impact of this new technology on the relation between people and their world, by its mediating role in this relation[9]. "The world" in this case means the political lifeworld of democracy. Technology may amplify or reduce certain aspects of experience, and invite or inhibit certain kinds of actions. Internet voting is not only a matter of "doing the same thing, but faster and more efficient". It touches the experience of voting fundamentally, and so the heart of our democracy[10].

We will provide an introduction into the ethical aspects of this technology, by studying the mediating role of voting technology in the relation between citizens and the political world of democracy. We start with discussing the basic problem of trust in technology. Trust plays an important role in the lifeworld of modern people, and it is not hard to understand that trust has gained importance against the background of the so-called "crisis" in democracy. We will point at irrational mechanisms that characterise trust, which can entail problems in the relation between citizens and state when expectations are too high. In the second part of this paper, the generally recognised minimum conditions for elections are presented, as expectations involved in the introduction of Internet voting technology. The aspect of vote secrecy is further analysed in relation to the changes in democracy that Internet voting brings. In the fourth part, more practical problems in the implementation of Internet voting systems are discussed, based on a case study.

We assume that Internet voting will be offered alongside existing voting procedures. Since not everybody can be expected to have access to the Internet in the near future, it is not a realistic option to do elections solely based on the Internet soon. Therefore, we do not discuss ethical issues of accessibility[11].

TRUST IN TECHNOLOGY

In democracy, as in all human action, "what is going on" is intersubjectively constructed from the "image" people have of what is going on[12]. Partly due to the huge importance of media in a democracy, the latter has its own dynamics. An important phenomenon in the constitution of this image is trust. It is not only important that a system is reliable, it is also important that people *believe* that the system is reliable. This is particularly important for voting systems against the background of the grown discomfort and the so-called crisis in democracy. For instance, it has been suggested that doubts about the anonymity of a vote might tempt the voter to vote more "politically correct"[13]. A technology that raises doubts about anonymity, whether justified or not, can change the relation between the voter and her world in such a way, that different choices are made. This means that designers and policy-makers not only have to make sure that the voting process is organised such that the anonymity of the vote is appropriately protected, but also that people have *trust* in the anonymity. In this section, we present paradoxes and risks that characterise trust in technology.

In recent years, in social sciences and ethics, there has been a remarkable growth in the literature about trust. This has been accompanied with a growing appreciation of trust. But what is trust? The most general and therefore least controversial definition derives from Simmel: 'a blending between knowledge and ignorance'. On one hand it implies more than naively hoping things will be going well. Trust does not arise spontaneously; it is a rational decision in the sense

[9] Ihde (1990) and Verbeek (2000)

[10] The relation between democracy and technology has also been addressed from the opposite direction: how do we make sure that technology is developed according to democratic values? See Sclove (1995) and Harbers and Bijker (1996).

[11] There is a more subtle moral issue involved here when we require completely equal access, in terms of equal costs of casting a vote for all voters (Cunningham, 2002: 105-106). We will not discuss this issue here.

[12] Berger & Luckmann (1967)

[13] Oostveen & Van den Besselaar (2003)

that a person considers situations carefully[14]. On the other hand, one does not have the capacity to make a complete estimation, and therefore has to “trust”. Trust differs from certainty. It requires some knowledge but accepts that complete knowledge can not be given. It enlarges the willingness to take risks but is not a blind “jump into the unknown”.

An important merit of trust is the fact that it reduces complexity and so opens possibilities for action. Luhmann, who considers this as the most important characteristic, describes how the world for the individual presents itself as an unmanageable complexity. The future contains many more possibilities than can ever be realised. In trust, the individual envisages certain (future) events. It enables her to recognise uncertainties[15] but at the same time set priorities and make choices.

However, the inevitability of a simplified image of the environment implies a tension that finds expression in the fragility of trust[16]. Trust usually exists in a self-evident way, based on the generalisation of experiences. People extend experiences to similar cases, and stabilise indifference to variation. Generalisation means that the environment is seen as a more or less coherent whole. Luhmann talks about ‘symbol complexes’ that are trusted. As long as there are shared understandings and common experiences, trust is implicitly confirmed. As soon as the need is felt to make existing mechanisms of trust more explicit, the self-evidency is lost and distrust is creeping in. This clearly shows the fragile character of trust. By subtle social mechanisms it can be easily harmed. Small mistakes can have devastating consequences.

These properties of trust not only apply to trust in the social sphere, but also to what Luhmann calls ‘system trust’. This kind of trust does not apply to interpersonal relations, but to the functioning of a certain socio-technical system as a whole. System trust implies renouncing, as a conscious risk, some possible further information and continuous monitoring of results. It is a necessary precondition for a technological society. One may expect trust to be increasingly in demand, as a means of enduring the complexity of the future that technology will generate.

There are intriguing processes at work in system trust. In certain respects system trust is, more than social trust, a “jump into the unknown”. By definition a rationality is accepted that cannot be understood. Contrary to trust in a person’s character, is it impossible to make a serious estimation of the reliability of the system. The experts that are familiar with the workings of (parts of) the system may present many technical arguments that can be understood by their fellow engineers, but their fellow citizens will never understand them. The citizens’ decision to trust the engineers touches a different dimension, which cannot be understood and justified completely in rational terms. The attitude involved comes closer to “belief” in the authority of people. This can unexpectedly and quickly turn towards its opposite. In this way a high level of trust can change into severe disappointment and grave distrust.

The definition of trust as a blending between knowledge and ignorance might suggest that, as far as we approach knowing, there is a diminishing need for trust. However, there is no exact congruence between growth of (objectively seen) convincing arguments, and reduction of trust. First, because a complete congruency between trust and “objective merits” does not do justice to the phenomenon of trust. Trust just arises in situations where it is hard to determine exactly the results of actions. Moreover, the history of the introduction of technical systems shows sharp incongruities in the relation between rational planning and trust. Some technical systems have been accepted and trusted in spite of serious disadvantages. The naive acceptance of voting machines in the Netherlands can count as an example. When the machines were introduced in the early nineties, there was hardly any discussion about their reliability and the possibilities for public verification of the counting process. But the computer programs used in them are not available for public review.

[14] Waterval (2003): 38

[15] ‘Trust increases the tolerance of uncertainty.’ (Luhmann, 1979: 15)

[16] Luhmann (1979): 26

Isn’t this a violation of the citizen’s right to verify the voting process completely?[17] People did not worry because there was a high level of trust in technology and the Dutch government. On the other hand, systems that complied to high safety standards have met distrust. Experts might, in their own terms, give very sophisticated answers, but still people do not necessarily trust them.

Again, the acceptance of technical systems turns out to be embedded in a social context. It depends on the experience and perception of people. In this perception, there is a serious difference between trust and a passive attitude. On the surface they seem to lead to the same kind of actions, but trust is a more stabilising attitude, whereas passivity of citizens is problematic. In the latter the citizen is indifferent, even when her own interest is at stake. The unstable character of passivity gets clear when the citizen turns into protest and obstruction. When this stage has arrived, it is often too late to repair things.

In ethical considerations concerning voting, we have to pay attention to trust in order to preserve the stable character of democracy. Paper voting has earned a large amount of trust in the experience of citizens, partly due to the well-organised social context. Progress in technology should not lead to problems with democratic progress in society, which may easily become the result of distrust in the election system. If voting technology mediates the relation between people and democracy in such a way that the experience of trust and stability is reduced, for whatever reason, the actions that are invited are political passivity on the one hand, and protest and obstruction on the other.

PRINCIPLES OF VOTING

Some principles have been established to guarantee the proper functioning of elections in our democracy. These principles should make sure that the goal of elections in representative democracy - i.e. establishing a parliament that forms a representation of the people based on some country-dependent calculations - is achieved. For this reason, they are also the principles that confirm the identity of our democracy. Although they are subject to discussion and have to prove their value in practice, they cannot just be discarded if they become inconvenient at some point. The social role of these principles is that of expectations[18] that the involved actors acquire based on current practices and institutions. If these expectations are not met by the voting technology used, this may have major implications for trust in the election system, via the mediating role of technology in the experience of people.

Based on McGaley & Gibson (2003) and Knoppers (2005), we can distinguish the following principles of elections:

- Correctness of the results
    a. Only eligible users vote;
    b. They only vote once;
    c. All votes counted are valid votes, and all valid votes are counted.
- Verifiability of results by involved parties
- Secrecy of votes

[17] Another example: in the days after the presidential elections in the Unites States in 2000, results of a research group of Berkeley University showed consistency between paper ballot results and exit poll, but a serious contradiction between electronic ballot results and exit poll. It is not the place here to discuss the validity of these results. It might be true what the New York Times wrote November 5 that year, that the discrepancy was the fault of the exit pollsters. For us it is important that these remarkable data did not arouse much protest. It turned out that people trusted the election system and could not believe that it had something to do with “the most massive election fraud in the history of the world”. See http://www.truthout.org/docs_04/110604Z.shtml, consulted April 27, 2005. See also Jacobs (2003).

[18] Weber et al (1999)

a. No one should be able to derive a relation between the vote cast and the involved voter (preventing forced voting);
b. A voter should not be able to prove which vote she cast (preventing sale of votes).

In paper voting, the conformation to these principles is achieved via *voter identification*, *supervised voting* and *distributed counting procedures*. People are admitted to the polling station only once, and they only get one opportunity to cast their vote. It is also hard to add invalid ballots to - or remove valid ballots from - the ballot box unseen. The paper system uses separate counting sessions in the different districts, and allows any citizen to attend the counting process, and thereby verify the result. Moreover, since voting is done under supervision of the election officials, you will be guaranteed a private voting environment. This is a warrant for the secrecy of your vote.

Via these aspects, paper voting has acquired a large deal of trust in the experience of citizens. Still, the ease with which this system has been replaced in the Netherlands suggest that there are other factors involved as well. One may argue that the electronic voting machines currently in use have been accepted based on passivity rather than trust. When these machines were introduced in the Netherlands, there has not been much debate about the conformation to the aforementioned principles. Instead, their introduction has been more or less tacitly accepted - in spite of decreased transparency - which is typical of passivity.

In the discussion on voting via the Internet, these principles should be taken into account to avoid a similar situation. Lack of conformation to and discussion about these principles might change the relation between citizens and democracy in such a way that aspects of trust are reduced in their experience. In that case, passivity is not only misused as an easy way to change the system, but also invited as future behaviour. Below, we will discuss the issues that are involved concerning these principles when this new technology is used in elections.

Only eligible users vote

To be able to vote, voters should carry some unique identifier that can tell the system that they are allowed to vote. In regular elections in the Netherlands, voters are sent an "oproepkaart" by mail that they have to hand in at the polling station. The operators of the polling station may ask for additional identification as well, although this is not often done. In the online case, procedures are similar, except for the fact that it is hard to ask for additional identification online. Voters are given an *access token* (e.g. a password or a chipcard) that they can use to cast their vote. One of the issues is the ease with which this token can be transferred. Transferring a token means giving your vote to somebody else, which can be under pressure or in exchange for money. Easy transfer thus means easy fraud. A password can be sent electronically, whereas a chipcard must be physically transferred.

They only vote once

People should not be able to cast more than one vote in the election process. This means two things: first, people should not be admitted to the election more than once, and second, people who are admitted to the election should only be able to vote once. The second condition is relatively easy to fulfil in an electronic case. If the program only allows one vote per voter, and votes cannot be added without using the program and appropriate access tokens, then we are done. The first condition, however, is difficult, because people may give their access tokens to a different person, who can then vote more than once using different tokens.

All votes counted are valid votes, and all valid votes are counted

In elections, all valid votes, and only valid votes, should be counted. It should therefore not be possible to add or delete votes by bypassing the identification procedures. Moreover, ballots on which multiple candidates are selected for the same position should be declared invalid. Especially noteworthy in the Internet case is the protection of the servers that receive the votes. If people who have access to a server that registers votes can also access the database and add or delete votes, then this condition will not be fulfilled.

Verifiability of results by involved parties

The voting machines currently used in the Netherlands and many other countries are not particularly suitable for verifiability. In the transition to voting machines in the Netherlands, it has been tacitly accepted that we cannot verify electronic votes. People seem to accept the system anyway, although discussion in other countries also leads to questions here. In Ireland, the same machines were purchased but never taken into service, because there was no possible way to know that they calculate the results correctly[19]. Researchers are arguing for 'Voter Verified Audit Trails', which means that the voter's choice is printed on a paper, which can be inspected (behind glass) and is automatically dropped in a ballot box afterwards. This enables manual recounts, if there are any doubts about the results.

Some researchers state that secure Internet voting is impossible, because it cannot be implemented with a paper audit trail. Actually, there are some interesting new possibilities for verification in Internet voting, which we will discuss later.

Secrecy of the vote

The demand of secrecy makes voting a much more complex process to implement online than other services. In online banking, you should authenticate yourself in order to gain access to your account. All transactions will be linked to you. In voting, you should authenticate yourself in order to be able to cast your vote, but the transaction should *not* be linked to you. Otherwise, people who are interested in your vote may be able to derive who you voted for, and take appropriate measures.

In Internet voting, the secrecy condition cannot be fulfilled the same way as in the polling station. There are indications that with Internet voting major concessions are made in this matter. In order to judge how bad this is, we must look at the importance of secrecy for voting in a democracy. We will describe the implications of this problem for the relation between people and democracy next.

HOW INTERNET VOTING CHANGES DEMOCRACY

Because of the dynamics of mediation in relation to trust, Internet voting can change the intersubjectively constituted image of voting and democracy. In this section, we investigate the most fundamental issue that is related to this mediating role of technology. Voting carries one particularly important aspect of democracy: the tension between public and private[20].

There has been much debate on the question what the essence of democracy is. In political philosophy there is a wide range of democracy-theories[21]. Some stress the importance of basic rights and liberties, others mechanisms of institutional representation. But all agree that democracy is the best political solution for the problem of dealing with diversity of opinions and interests. This

[19] http://evoting.cs.may.ie, consulted April 14, 2005

[20] See e.g. Heysse & Goossens (2003).

[21] See e.g. Cunningham (2002).

requires a delicate balance between personal and public matters. Personal convictions and individual preferences are presented in a public space that is filled with discussion and debate. Politics has to do with "making visible": showing to the public and exchange of opinion[22].

In recent years, a growing awareness has developed that this not only requires formal institutional arrangements. Institutions only function in a dynamic relationship with the appropriate mentality. In all democracy theories, it is recognised that at least a minimum of a positive attitude towards discussion and deliberation is required. It is a danger for democracy when the citizen retires in the private sphere. As Tocqueville 150 years ago already concluded: in modern commercial society, there is a real threat that people will become indifferent to politics, or lack political energy. This may be a source of political corruption. Social life will be characterised by a sort of "civic privatism": 'a reflective and peaceful sentiment that disposes each citizen to draw herself off to the side with her family and her friends, in such a way that, after having thus created for herself a small society for her own use, she willingly abandons the larger society to itself'[23].

The words of Tocqueville are often referred to as if they had prophetic power. A diminishing involvement of the democratic citizen is a real threat to democracy at this moment. The Flamish sociologists Elchardus and Smits convincingly showed that a growing number of citizens are alienating from the discussion-and-debate culture. They distrust not so much institutions in which professionals work with their particular skills, but particularly those institutions that are set up to arrange public discussion. The distrust towards democratic institutions is accompanied by a pessimistic view on mankind in general and politicians in particular. They are considered to be selfish; their noble words about public interest are only a disguise to enrich themselves. To people with these convictions public debates are wasted[24]. As they are suspicious towards "parliamentary quarrels", they prefer the strong hand of the populist leader[25].

Against this framework it is important that Internet voting mirrors a paradoxical shift in the public-private balance. In the polling station, voting is a "public act", in the sense that an individual contributes to public decision-making. But it is done in exclusion. This is not just a pragmatic choice in effect, but has an intrinsic value for the democratic process in the way in which the individual experiences the act of voting. Completely alone, thrown upon her own resources, the individual has to decide. The act of voting mirrors citizenship: left alone with its particular ideas and preferences the subject knows herself part of a larger process. In this sense, voting has a "ritual" character: seemingly trivial gestures that have a huge meaning for those involved.

Especially important in this ritual is the offer of a moment of secrecy. The secrecy of elections is explicitly mentioned in the Dutch law[26]. State and society take great pains and costs to guarantee that the citizen is left alone during voting. Polling stations are equipped in such a way that people vote in isolated corners. There is an interesting paradox at work here: in the public domain the authorities guarantee a moment of privacy and secrecy.

This delicate balance between public and private changes fundamentally in Internet voting. In Internet voting, people are free to choose the place where they want to vote. Probably most voting will be done at home or at work. If people vote at home, voting seems to be a private matter again. Isn't the inner circle of the home the summit of privacy? The answer is no. In the atmosphere of the home, absolute exclusion is not guaranteed. When people vote at home, there is no guarantee that

[22] Most convincingly elaborated in the work of H. Arendt. See for instance Arendt (1972) and (1958).

[23] Quotation in Honohan (2002): 113

[24] Elchardus and Smits (2002).

[25] Idem.

[26] http://web.inter.nl.net/users/sf/kieswet.html, consulted April 15, 2005. Kieswet (Dutch election law), Section J 15: 'Het stemlokaal is zodanig ingericht dat het stemgeheim is gewaarborgd.' ('The layout of the polling station guarantees the secrecy of the vote.') Section M exhaustively describes the exception: voting by letter (particularly for those citizens who stay abroad).

others do not look over their shoulders to make sure that they make the "correct" choice. It even allows for both vote coercion and vote sale. We have to admit that complete secrecy is impossible at home[27]. Those who deny the importance of this, show an all too naive trust into the autonomy of people.

From a fundamental perspective, this may be understood as disastrous to democracy. If people are able to sell their votes or force others to vote for a certain party, even in limited numbers, democracy is destroyed. However, there are other means to avoid these excesses, apart from physically guaranteeing a moment of secrecy. Organisational and legal measures have always been important in democracy, and a balance may be found in this matter as well. We will not discuss the details of these possibilities in this paper, but we do recommend political discussion on this topic[28].

The lack of secrecy at home is not only important for the organisational and legal context of elections, but also for the way in which people understand democracy. In an ironic formulation we can say that, whereas at the polling station voting is experienced as a "private moment" in a public surrounding, Internet voting introduces a "public moment" in a private surrounding. This may reduce the aspect of voting as part of a larger public process in the experience of people. This will have implications for the way people understand democracy, and we have to discuss these implications before we introduce the technology on a large scale.

RULES FOR DESIGNING INTERNET VOTING SYSTEMS

In the previous sections, we discussed how Internet voting may change democracy. Internet voting cannot meet all expectations based on paper voting, and it changes the act of voting in the experience of the citizen. Both of these aspects, if not carefully considered in political discussion, may decrease trust in democratic institutions. If we want to adopt Internet voting anyway, we have to be careful about the choices we make in its implementation, since the properties of the concrete system will have influence on the relation between citizen and democracy as well. In this section, we will discuss these issues.

The complexity of the task makes online voting an interesting research challenge for computer scientists, and various proposals for solutions can be found in the literature. Unfortunately, many of the solutions are hard to understand even for computer scientists, let alone for the public[29]. Our case study, the RIES system developed for the online elections for the "waterschappen" (public water management authorities) of Rijnland and Dommel in the Netherlands, is an example of a system where things are kept reasonably simple[30]. We therefore think that it is a good candidate for future elections, with some adaptations.

The RIES system was developed by the "Hoogheemraadschap van Rijnland"[31] and MullPon vof[32]. It was considerably cheaper than comparable systems, such as the KOA system[33] designed to allow Dutch citizens staying abroad during the European Elections 2004 to vote via Internet or phone. It worked well in two elections with over 2 million potential voters. More than 120 000 votes were received via the Internet. About 280 000 people chose to vote by ordinary mail.

[27] This aspect is also known as "family voting".

[28] Actually, some secrecy has already been sacrificed by the abolishment of the obligation to vote in the Netherlands in 1970. Whereas your vote is still secret *if* you vote, whether you vote or not is now public information and therefore subject to manipulation.

[29] See e.g. Joaquim et al (2003) for an overview and an example system.

[30] The empirical material consists of documentation and participation in the evaluation process of the systems. The analysis of this material is based on the theory of Strategic Niche Management (Weber et al, 1999).

[31] http://www.rijnland.net, consulted April 15, 2005

[32] http://www.mullpon.com, consulted April 15, 2005

[33] http://www.minbzk.nl/persoonsgegevens_en/kiezen_op_afstand, consulted April 15, 2005

According to the designers, this has been the largest formal Internet election on the planet so far. We are not aware of any experiments with higher figures.

In this section, we will discuss choices that have to be made in the technical design of online voting systems, and their ethical implications. We will discuss some risks[34] involved in online voting, and we will explain how the RIES system tackles these issues[35]. After this, we will summarise our recommendations. We will see that gaining trust in such a system requires a delicate balance between conflicting values.

"I think my vote has been registered incorrectly; can we please redo the elections?"

One of the issues worth discussing is whether it should be possible for voters to verify their vote after the result of the elections has been published. The most basic argument says that this should not be allowed, since it constitutes proof of a vote. The traditional demands posed on elections prohibit this, because of the possibility of vote coercion and vote selling. If it is possible for a voter to prove what she voted for, then an attacker may demand this proof (or else….).

However, in online voting this is a less important issue. Because people vote at home, and others may watch them vote anyway, it does not really matter if they get proof of their vote afterwards. If an attacker wants to force them to vote for a specific candidate, she may as well force them to give her their access token. The ethical reasoning involved here is that if we change the voting system in a fundamental way such that certain properties do not hold anymore, we do not need to keep measures that are meant to guard those properties either.

In the RIES system, it is possible to verify your vote after the elections. Because of clever use of certain cryptographic techniques, you can check whether the vote registered under your own access token (in this case a voter code and a password) maps to the right candidate, and given all registered votes, you can calculate the result yourself. You will need to write a computer program for the latter purpose, but in principle it is possible[36].

The question is of course whether these kinds of checks are enough to protect the integrity of the elections and trust in the result. If only a small fraction of the voters do indeed verify their votes, then a major flaw in the results might still go unnoticed. Moreover, since only computer-literate people will be able to do independent calculations of the result, it may be argued that it is not really a democratic way to protect the elections. The danger of "elitism" involved also directly touches the trust. People might consider it as a confirmation that only technical experts "rule the system".

On the other hand, the current elections do not even allow for vote checking and full independent recount at all. Recounting is especially intricate when voting machines are involved. The vote stored in the machine at the time of voting may already be different from the voter's intention, without any chance of detecting this. In this sense, online voting may even improve transparency, at the cost of a more complex election system, that may not be explainable to everyone[37].

[34] Jefferson et al (2004) argue that Internet voting cannot and should not be used in the near future, due to security problems. We take a more pragmatic view, and follow Alvarez and Hall (2004) in their opinion that more (scientific) experiments are needed to provide a good overview of problems and solutions.

[35] For more details about the RIES system, we refer to Jacobs and Hubbers (2004) and Hubbers, Jacobs and Pieters (2005). See also http://ww.rijnlandkiest.nl, consulted April 29, 2005.

[36] The Security of Systems group at the Radboud University Nijmegen did this for each election that used the RIES system (Hubbers, Jacobs and Pieters, 2005).

[37] There is another issue of transparency involved in electronic voting, namely whether the computer programs used should be available for public review (open-source). We will not discuss this issue in this paper. See Kitcat (2004) for more details.

Transparency is an extremely important value in democracy. We argue that in the online case, it is even more important than vote secrecy. We cannot guarantee complete secrecy if people vote at home, which makes it less important to implement measures that protect secrecy, if we want to vote online anyway. Complete destruction of the link between voter and vote after the act of casting is such a measure. We think that the option of vote verification (which requires keeping some information about the vote) is more attractive than trying to maintain secrecy where it is not possible.

This links directly with the mediating role of election technology in the relation between citizens and the state. If we provide technology that allows verification, we gain two things. First, people may become more actively involved in the election process if we allow them to do more than just click and wait. This invites active participation in the election procedure, as opposed to passivity. The experience of voting is extended by the verification procedure, which even may be considered a new kind of ritual. Second, even the option of verification being there, without the necessity of people actually verifying their vote, may change the experience of voting and amplify the aspect of trust in the system in this experience.

Online voting rule 1: Allow voters to verify their vote

Who will guard the guards?

If an online service is offered that allows people to verify their vote, this may be done by the organisation also responsible for publishing the result. However, this allows them to present a different vote to you than they used in the result calculation. This possibility was actually present in the experiments with the RIES system, and it is an example of a situation where the distribution of power is not taken care of well enough. Current elections are based on the principle that multiple actors are involved in all districts and at all stages, such that the opportunities for tampering with the results are small. In an online system, we would like a similar compartmentalisation, to prevent any party from getting too much power[38].

This directly touches the problem of trust. If an election system fails in this respect, and can only be managed and understood by a technological or political elite, it may mediate the experience of people in such a way that the interpretation of government as something elitist is amplified, and this may increase passivity. Although system trust requires people to accept that they do not understand everything themselves, trust also requires the conviction that things are taken care of by enough competent and independent people, and that there are possibilities for intervention if things get out of hand.

Online voting rule 2: Vote verification is not enough; distribution of power is still needed

"I didn't vote, my computer did"

A possible risk in online voting is the presence of a virus on the voter's computer. Such a virus might intercept the communication between the voter and the voting web-site, and thereby change the vote[39]. The question is whether it is the responsibility of the designers of the voting system to prevent these kinds of attacks. We might argue that each voter is responsible for the proper functioning of her computer system, since it is private property and not under public supervision. On the other hand, we can state that most users do not have the expertise to make sure that their

[38] A special concern in online voting is that insiders should not be able to *add* votes. The probability that someone who did not vote will check that there is indeed no vote registered in the results for her is very small.

[39] See e.g. Jefferson et al (2004).

system is clean. Then, the design of the voting system should include features that make it hard for viruses to change votes.

These means are available. Each user may get a different ballot, such that the codes for each candidate differ per user. In this way, a virus will not know how to change a vote in order to get a vote for the desired candidate. However, this requires more advanced interactions between the voter and the website. Moreover, different codes per user make the logistics of the system more complex: different ballots have to be printed, and the correspondence between the access token and the candidate codes needs to be stored somewhere. Because of these reasons (more difficult for the user, and more complex logistics) the designers of the RIES system chose not to implement these measures. The probability of this kind of attack was estimated low, and it was argued that a more complex system might decrease ease of use.

Although this may seem too easy a solution, the designers put their finger on a quite important feature of trust here. This feature of trust also showed itself in practice. The first version of the verification scheme in RIES was tested for usability. It was found that many users judged the procedure too difficult. Moreover, trust in the system seemed to *decrease* instead of increase if this kind of verification was offered. Apparently, trust in a system decreases if users are confronted with too many details of the inner workings, or too complex procedures. This can be explained in terms of the analysis we have presented, inspired by Luhmann. System trust, more than personal trust, relies on a deliberate avoidance of further information about the system. The willingness to trust is not directly proportional to the force of the arguments presented by experts. When the black box of the system is opened in the experience of the user, this may reduce her trust.

Based on the analysis by Luhmann, we can state that it is wise to pay attention to user-friendliness of the system, in order to enable system trust to do its work in the experience of the user. This may even mean that state-of-the-art cryptographic techniques should not be implemented if this reveals much more complexity to the user. By the implicit moral reasoning involved in the design of RIES - do not try to meet demands that are not realistic in the online case anyway - it can offer a verification scheme that is in principle reasonably simple and transparent. This, in turn, does not make it necessary to confront the user with all kinds of paranoid measures to increase security, since the system is verifiable anyway. And hereby, RIES allows for more system trust than a paranoid system, even if it may be less secure from a technical perspective.

This is not to say that any system that acquires trust is also a desirable system. But we do want to emphasise that lack of attention to usability in Internet voting systems may destroy trust in the whole idea, just by making things too difficult in the experience of the user. It also may lead to reduced trust in democratic institutions in general. This is another feature of the mediating role of technology in the voting process. Lack of usability can mean that interesting options to improve democracy will not be implemented, whereas a combination of technical and procedural measures is not unable to assure reasonably secure elections.

Online voting rule 3: Find a good balance between security and usability, since problems with either of these may destroy trust in Internet voting

In summary, we have the following three rules, based on our ethical considerations:

1. Allow voters to verify their vote;
2. Take measures to guarantee distribution of power, to prevent insider attacks as well as the experience of elections as an elitist matter;
3. Find a good balance between security and usability.

CONCLUSIONS AND RECOMMENDATIONS

In this paper, we presented a philosophical analysis of the changes and choices that Internet voting may bring to our democratic society. The issue of Internet voting is particularly pressing, because the demand for introduction of the technology is strong. It is strengthened by the mediating role of other online technologies. Because other services are offered via the Internet, the experience of people is mediated in such a way that the aspect of availability at home is amplified in people's understanding of a "service". This also applies to voting. The "why can't this be done at home?" argument exemplifies this mediation.

However, as we have elaborated, voting is something different from other online services. In Internet voting, the pivotal moment of democracy - voting - is experienced differently. This may not be surprising; the shifting public-personal balance mirrors a general development in present-day society[40]: publicly shared experiences give way to more private experiences on a smaller scale, where people are very susceptible to all kind of influences. Internet voting implies a loss of involvement with the public character of the voting process. Instead of a private moment in a public surrounding, voting now becomes a public moment in a private surrounding. Part of the ritual dimension is lost. Internet voting even implies an increased risk of undue influence on the voting process, due to lack of supervision. However, there are no indications that this will destroy democracy. Not everything depends on the technology used, and there are other means to enforce proper behaviour in elections and allow people to experience elections as part of a larger process.

Internet voting is not only a matter of collecting votes in a different way. The development of trust within the relation between citizens and democracy has its own dynamics and rationality. Because of the mediating role of technology in this relation, Internet voting can change the intersubjectively constituted image of voting and democracy, and thereby contribute to or destroy trust. Trust in the voting process, the technology used and democracy itself are interwoven. If we consider democracy as an important value, we have to make sure that new technology does not destroy this trust.

Since the technology is not neutral, not only the relation between citizen and state will be changed if we adopt new voting technology, but also the expectations people have about this technology should be considered critically. We discussed how existing principles of democracy, based on traditional paper voting, function as expectations of actors in experiments with Internet voting. Internet voting cannot meet all of these. But this is not a definitive argument against Internet voting. As far as security is concerned, Internet voting can only be reasonably compared to postal ballots. In both cases, there is a lack of control over the voting environment. Some elections are already completely run by (regular) mail, and there has been no evidence of extensive fraud[41]. Requiring the design of Internet voting systems to be compatible with demands that stem from a time when voting was experienced differently is not realistic.

We should assess the demands for the new democracy that we want. These new demands should provide a context in which the technology and the accompanying organisational and legal institutions for the new situation can be properly designed, taking ethical considerations into account, especially in relation to trust. Establishing these demands is a political task. We discussed some guidelines for the implementation of Internet voting, if this turns out to be the technology that we want. We showed that seemingly small aspects of the chosen Internet voting system may have major implications for the way in which people experience voting and understand democracy.

In social science, it will be useful to investigate the actual effects of voting at home. We are not aware of significant figures that indicate effects of an unsupervised voting environment on voting

[40] See also Sennett (1977).

[41] E.g. in Oregon in the United States, see Alvarez & Hall (2004): 113-119. Recently, the United Kingdom did experience fraud with postal ballots: http://www.timesonline.co.uk/article/0,,19809-1564522,00.html, consulted April 22, 2005.

behaviour. Also, the willingness of people to sell or buy votes in elections is still unknown. How many people would be likely to sell their vote if a market for votes comes into existence by relaxing control on the voting environment? And how strongly is behaviour in voting in relation to pressure (blackmail, threatening, etc.) dependent on the secrecy of the vote? Pressure from family members may quite well work, even if the vote is secret. Such figures will greatly improve our understanding of the risks of Internet voting, and can help to establish appropriate legislation.

In future research, we wish to investigate the effect of the advent of Internet voting on discussions on democracy. Internet voting may change existing ideas, and discussion may benefit from the challenges that Internet voting brings. More research is also needed in the area of trust, especially trust in information systems and the role of computer scientists and program verification technology in this area.

Internet voting is neither necessary nor inevitable, but we think society should make sure that it is ready for its adoption, since it may show itself to be an important feature of the new democracy of the information age.

ACKNOWLEDGEMENTS

The authors wish to thank (in alphabetical order) Bart Jacobs and Erik Poll for useful comments on drafts of this paper.

REFERENCES

Alvarez, R.M. and Hall, T.E. (2004) *Point, click & vote: the future of Internet voting*. Brookings Institution Press, Washington D.C.

Arendt, H. (1972) *Crisis of the republic; Lying in Politics; Civil Disobedience; On Violence; Thoughts on Politics and Revolution*. Harcourt Brace Jovanovich, New York.

Arendt, H. (1958) *The Origins of Totalitarianism*. Cleveland: World Publishing Company, Chicago.

Berger, P.L. and Luckmann, T. (1967) *The social construction of reality: A treatise in the sociology of knowledge*. Anchor books, New York.

Cunningham, F. (2002) *Theories of democracy: a critical introduction*. Routledge, London.

Dewey, J. (1991) *The public and its problems*. Swallow Press / Ohio University Press, Athens.

Elchardus, M., Smits, I. (2003) *Anatomie en oorzaak van het wantrouwen*. VubPress Brussel 2002.

Harbers, H. and Bijker, W.E. (1996) Democratisering van de technologische cultuur. *Kennis en methode*, **20**(3): 308-.

Heysse, T. and Goossens, W. (eds.) (2003) *Democratie als filosofisch vraagstuk*. Pelckmans, Kapellen.

Honohan, I. (2002) *Civic Republicanism*. Routledge, London.

Hubbers, E., Jacobs, B. and Pieters, W. (2005) RIES - Internet voting in action. *Proceedings of COMPSAC 2005* (to appear).

Ihde, D. (1990) *Technology and the lifeworld*. Indiana University Press, Bloomington.

Jacobs, B. and Hubbers, E. (2004) Stemmen via internet geen probleem. *Automatisering Gids*, 2004(42): 15-.

Jacobs, B. (2003) *De computer de wet gesteld*, oratie. Katholieke Universiteit Nijmegen.

Jefferson, D., Rubin, A.D, Simons, B. and Wagner, D. (2004) Analyzing Internet voting security. *Communications of the ACM*, **47**(10): 59-64.

Joaquim, R., Zúquete, A. and Ferreira, P. (2003) REVS - A robust electronic voting system. *IADIS International Journal of WWW/Internet*, **1**(2).

Kitcat, J. (2004) Source availability and e-voting: an advocate recants. *Communications of the ACM*, **47**(10): 65-67.

Knoppers, P. (2005), *Stemmachines? Niet doen!* http://ce.et.tudelft.nl/~knop/stemmachines/, consulted April 14, 2005.

Luhmann, N. (1979) *Trust and power: two works by Niklas Luhmann*. Wiley, Chichester.

McGaley, M., and Gibson, J.P. (2003) *Electronic voting: a safety critical system*. http://www.evoting.cs.may.ie/Project/report.pdf, consulted April 14, 2005.

Oostveen, A.M. and Van den Besselaar, P. (2003) E-voting technology is not neutral!, in Dittrich, K. et al (eds), Informatik 2003, Innovative Informatikanwendungen, Band 2. *Lecture Notes in Informatics* P-35: 218-221.

Oostveen, A.M. and Van den Besselaar, P. (2004) Internet voting technologies and civic participation: the users' perspective. *The public* **11**(1): 5-.

Sclove, R.E. (1995) *Democracy and technology*. The Guilford Press, New York.

Sennett, R.(1977) *The fall of public man*. Cambridge University Press.

Verbeek, P.P.C.C. (2000) *De daadkracht der dingen*. Boom, Amsterdam, 2000.

Waterval, D. (2003) Vertrouwen, in: Balkenende e.a. (red.), *Onderneming en maatschappij. Op zoek naar vertrouwen*, Koninklijke Van Gorcum, Assen.

Weber, M. et al (1999) *Experimenting with sustainable transport innovations: a workbook for strategic niche management*. University of Twente, Enschede.

BIOGRAPHIES

Ir. drs. Wolter Pieters is junior researcher in the Security of Systems group at the Radboud University Nijmegen. He studied computer science and philosophy of science, technology and society at the University of Twente. The topic of his current research is the achievability of Internet voting, both from technical and social perspectives. Dr. Marcel Becker is assistant professor philosophical ethics at the Radboud University Nijmegen. He studied history and philosophy. The topics of his research are particularly ethics of public administration, business ethics, media ethics and ethics of war and peace.