In: U.E. Gattiker (Ed.), *EICAR 2004 Conference CD-Rom*.
Copenhagen: EICAR e.V. ISBN 87-987271-6-8

Ask No Questions and Be Told No Lies

Security of computer-based voting systems: user's trust and perceptions

Anne-Marie Oostveen & Peter van den Besselaar

Department of Social Sciences, NIWI- KNAW
Royal Netherlands Academy of Arts and Sciences.
anne-marie.oostveen@niwi.knaw.nl
peter.van.den.besselaar@niwi.knaw.nl

Abstract

In this paper a pilot e-voting system is being studied in order to gain insight into the complexity of IT security issues. The current debate about whether or not electronic voting systems need to have a verifiable paper audit trail provides the context of the paper. Contrary to public perception, there is a long history of technical "glitches" and irregularities involving voting machines. According to many researchers a voter-verified paper audit trail is the only way voters can have confidence that their vote has been recorded correctly each time, and that recounts and spot checks are possible. However, more and more well-known technologists acknowledge that security mechanisms are fundamental social mechanisms. In all of this the issue of trust is of great importance; people no longer have a blind faith in scientific objectivity and do no longer trust the "experts". In this paper we will examine the opinions of users involved in the testing of the TruE-Vote electronic voting system, in particular concerning issues like security, verifiability and trust. The results do indeed suggest that IT security is more than just a technological issue.

1. Introduction

In an attempt to modernize our election process by moving from paper ballots towards the world of digital computers, governments might be jeopardizing our democracy. Many politicians and legislators are in favour of electronic voting. They see many possibilities in this new technology. Most proponents of electronic voting argue that the adoption of such systems would increase voter participation, especially among youths, overseas personnel, business and holiday travellers, and institutionalised or house-bound voters. Increasing voter participation is of interest because voter turnout has been low and declining in most countries. Election directors are also quick to pick up on the argument that electronic voting may be the cheapest and most efficient way to administer elections and count votes. Tedious duties such as counting every ballot twice and double-checking the process to avoid human errors cost millions. However, the cost of online voting would vary enormously depending on the type of system employed and the type of security used such as passwords, software, and biometric identification (Coleman et al., 2002). Electronic voting will also be the quickest way to count votes. If votes are cast online the results will be known within minutes after the election.

But from the first trials with e-voting onwards, there has been a lot of concern about the security of computer-based voting systems. Online voting systems have a lot of technical vulnerabilities. Already in 2000 the California's Internet Task Force concluded that the 'technological threats to the security, integrity and secrecy of Internet ballots are significant'. The general feeling was that although electronic voting is nice in theory, the security is still not sufficient. The British Independent Commission on Alternative Voting Methods also published a report recommending a delay of Internet voting until suitable security criteria are in place (Coleman et al, 2002).

Computer-based voting systems have to satisfy a number of criteria in order to guarantee a democratic election which is free, equal and secret. Broadly speaking, each election involves four distinct stages. First of all there is the registration of the voter. Prior to the election the voters prove their identity and eligibility. An electoral roll is then created. The second step is the validation. During the election, voters are authenticated before casting their vote. Only one vote per voter is authorized. After that the voters are allowed to cast their vote. Finally, there is the tallying stage. At the end of the voting period, all votes are counted. Each of the above stages can take place by using physical or electronic procedures. As said before, to design an e-voting system that can be used for large-scale elections, it is important to identify a set of publicly acceptable and technologically neutral criteria (IPI, 2001). Firstly, the election has to be democratic. Only authorized voters should be able to vote. A voter registration system should verify the voters eligibility (i.e. determine citizenship, age, legal residence, and that the person is still alive), and no voter can cast more than one vote. Secondly, the election needs to be accurate. Votes may not be altered, duplicated, or removed undetectably, nor should invalid votes be tabulated in a final tally. Election systems should record votes correctly. Thirdly, the election needs to be private. All votes remain secret while the voting takes place, and each individual vote cannot be linked to the voter who cast it. The fourth criterion is non-coercibility. No one should be able to determine how any individual voted, and voters should not be able to prove how they voted (which would facilitate vote selling or coercion). Finally, the public confidence in the election process depends on the verifiability and auditability of an election. There must be assurance that all votes cast are indeed counted and attributed correctly. As each vote is cast, an unalterable record must be created ensuring a verifiable audit trial (reliable and demonstrably authentic election records).

In this paper we focus on the criterion of verifiability. Public confidence in the manner in which ballots are counted is fundamental to the legitimacy of the electoral process. Electronic voting is likely to lead to changes in how the public maintains confidence in the integrity of elections. Internet systems pose a problem in that the tallying process is not transparent. With electronic voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process (IPI, 2001). Media stories about various

security threats to the Internet have an immediate impact on public confidence and past failures have made people distrustful. Electronic voting may not achieve the goal of increasing turnout if voters do not trust it. There are many ways to make electronic voting more secure. Mechanisms that form the structure of security are for instance Personal Identification Numbers (PIN) or passwords, encryption, digital signature, smart cards or biometric identifiers. It is important to make the voting and counting processes as transparent as possible. Because of this transparency there will be a greater confidence in the process and the result. Trust in an electronic voting system means having confidence in the machinery and infrastructure, rather than simply in the physical and administrative processes. All non-free software is secret by nature and there is virtually no way to be sure that the software does not include a trick to change the results of the vote. As McGaley and Gibson (2003) point out, 'apart from the obvious requirement that the votes are tabulated correctly, it is vital that the votes are seen to be tabulated correctly. A voting system is only as good as the public believes it to be'. A relatively simple way to provide a voter-verified physical audit trial was proposed by Rebecca Mercuri. Her method requires that 'the voting system prints a paper ballot containing the selections made on the computer. This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises. If, for some reason, the paper does not match the intended choices on the computer, a poll worker can be shown the problem, the ballot can be voided, and another opportunity to vote provided' (Mercuri, 2001).

Unfortunately, most of the electronic voting machines presently used in different countries do not provide a paper trail that can be compared to the machine count. So a recount is as good as impossible. Bev Harris's research shows that there have been numerous voting machine errors. All these errors came to light by accident when voters' rolls were compared with voter tallies and the numbers didn't add up, i.e. the number of votes cast did not match the number of voters who had signed in. Harris says: "Because hardly anyone audits by comparing actual ballot counts with machine tallies, we are not likely to catch other kinds of errors unless something bizarre shows up" (Harris, 2003: 33). She continues to point out how frightening it is that for every machine miscount discovered, there must be a hundred that go unnoticed. This impossibility to find out whether a machine counted the votes accurately is a major security issue.

No matter how undisputable the importance of technological security solutions (like voter-verifiable audit trails) are for gaining the trust of users, we think it is also indispensable to look at the more sociological issues that are at play. It goes without saying that a voter-verifiable audit will improve the trust of people in electronic voting systems, but history has shown us that trust in a new technology an sich is not sufficient for its success and adaptation. Neither can we state that trust in technology is always based on the actual state of the

technology itself. In this paper we will show that the opinion of users about the security of systems is often based on perception and not so much on actual facts. In other words, people will use insecure systems if the feel or think they are secure. They base this perception of security on things like: the reputation of the organizing institution, the attitude of the mass media, the opinions of friends and family and the convenience it will bring them. This paper tries to point out the importance of the socio-political context. Software may reduce the amount of trust you need in human beings, but as one moves about in the world, the sense of security, privacy and autonomy turns out to be "a function of social structures" (Ullman, 2000). This is an explorative study and it is not our goal to explain the opinions of users about the verifiability of the TruE-Vote system. We try to show that the belief in verifiability is not based on the technology itself but is more an issue of trust and opinions about new technology.

2. Voter-verifiable electronic voting

> "*Providing a voter-verifiable audit trail should be one of the essential requirements for certification of new voting systems."*
>
> David L. Dill, 2003

People should not just be able to vote, they should also have a voting system that can be trusted. If citizens don't trust that the elections they participate in are fair and the machines count right than they will never accept that those votes represent their voice. It is therefore that most computer scientists, social researchers and engineers are promoting a hybrid system. They favour touch screen machines with a voter-verified paper ballot, with an audit that compares the two against each other. With electronic voting systems there is always the risk that a program flaw or tampering with the software could change votes and even change the outcome of elections. And these changes may not be detected because of the secrecy of the vote. Since ballots are secret, once the voter has cast his ballot and left the polling booth, no one will be able to detect or correct possible errors that the machine made in recording the votes. Computer scientists say that the solution is relatively simple; all voting equipment should require a voter verifiable audit trail which provides a permanent record of each vote. This way the voter can check to ensure that it represents their intent. The free e-democracy project describes the way e-voting should be run in the future. The first step is that a voter casts his vote through a computer and clicks to send it. At this point the vote he wishes to cast is printed and checked by the voter. If the vote on the computer and that on the slip of paper matches than the voter continues. Otherwise he discards both and contacts an official. The paper votes are then deposited in a secure place such as a ballot box. It is vital that the voter

doesn't keep the paper so that he can't prove to someone that he has voted a certain way and get paid for it (Kitcat, 2003). When there is any doubt about the results of the election, there is the possibility of a manual recount. Without this requirement it would be impossible to have the confidence that our elections reflect the true will of the voters.

There are three reasons why the discussion about the security of electronic voting systems seems to have focused lately on the necessity of a voter-verifiable audit trail. First of all, the discussion about the need for voter-verified systems got a great impulse after the Florida election debacle, when the Institute of Electrical and Electronics Engineers (IEEE) took up the question of standards for voting equipment. The IEEE created a working group, called Project P1583. Unfortunately, instead of using this opportunity to create a good national standard, which would set benchmarks for the security, reliability, accessibility and accuracy of these machines, P1583 created a weak standard that would have led to unsafe electronic voting machines (Manjoo, 2003b). Even more problematic, the standard failed to require or even recommend that voting machines be truly voter verified or verifiable, a security measure that has broad support within the computer security community. A number of respected scientists involved in electronic voting were so appalled by the proposed new standard that they urged IEEE members and others to write to IEEE to express concern about their draft electronic voting machine standard. They warned that the future of democratic systems in the U.S. and around the world would be implicated by this standard. They stated: "We also support the idea of modernizing our election processes using digital technology, as long as we maintain, or better yet, increase the trustworthiness of the election processes along the way. But this standard does not do this, and it must be reworked." (Manjoo, 2003b). The main thing that has to change about the proposal according to these experts is that it should provide voter-verification. The point of the verified voting systems is that they preserve anonymity while providing two benefits: voter verification, and an ability to create a check on the machine. If the machine count and a count of the verification printouts don't match, then something is amiss. Without a form of voter-verification this would not come to light.

A second reason why more and more scientists started to worry about electronic voting systems without voter-verification was the uproar about the Diebold voting system. Numerous reports have found Diebold machines and other computer voting systems vulnerable to error and tampering (Kohno et al, 2003; Harris, 2003; Konrad, 2003, Manjoo, 2003a, 2003c). In general, no one is allowed to see the code used by electronic voting machines. Computer scientist David Dill says that when he started asking questions about voting machines, he received answers that made no sense. "It is frustrating because claims are made about these systems, how they are designed, how they work, that, frankly, I don't believe. In some cases, I don't believe it because the claims they are making are impossible" (Harris, 2003: 120). Dr. Dill is limited in his ability to refute the impossible claims because of

the secrecy of the data; machines can't be examined and manuals can't be looked at. Computer technician David Allen says: "These things are so secret we're supposed to just guess whether we can trust them" (ibid.). But lo and behold! More or less by mistake Diebold, the major manufacturer of e-voting systems published the source code of their system on a public internet site. Bev Harris discovered that Diebold's voting software is so flawed that anyone with access to the system's computer (the election supervisor, their assistants, the IT people, the janitor) can change the votes and overwrite the audit trail without leaving any record (Manjoo, 2003c). But someone could also get in to the system by hacking the telephone system or by going backwards in through the Internet (ibid.). This security flaw was already brought to light in October 2001 by Ciber Labs but Diebold did nothing to fix it. Even worse, a memo written by Ken Clark, an engineer at Diebold, says that they decided not to put a password on this system's 'backdoor' because it was proving useful. They were using the backdoor to do end runs around the voting program. After the election Diebold had "scrubbed clean the flash memory and gotten rid of the small cards that store the results from each touch-screen machine" instead of hanging on to the data for 22 months which is customary with paper ballots (Manjoo, 2003c). Scientists at John Hopkins and Rice also found that the security in Diebold's voting software was "far below even the most minimal security standards applicable in other contexts" (Kohno et al., 2003). Their report shows that worries about insider threats are not the only concern, but that outsiders can also do the damage (ibid). To summarize, by investigating the Diebold source code, the researchers found that voters can easily program their own smart cards to simulate the behaviour of valid smart cards used in the election. Also, undesirable modifications could be made by malevolent poll workers or maintenance staff before the start of the election. Furthermore, because of the lack of cryptographic techniques in the protocols, even unsophisticated attackers can perform untraceable "man-in-the-middle" attacks. Finally, a developer could easily make changes to the code (by inserting arbitrary patches) that would create vulnerabilities to be later exploited on Election Day (Kohno et al., 2003: 4). In reaction to the security issues identified by computer scientists, Diebold claims that the John Hopkins team is not very familiar with the election processes, makes false technical assumptions, has an inadequate research methodology and makes insufficient use of input from election experts (Diebold Election Systems, 2003, Kohno et al., 2003). The voting machine vendors furthermore state that researchers should have reviewed all the different layers of security in voting systems together. Sequoia Voting Systems for instance believes that: "Election security must be viewed as a combination of numerous layers of security that, taken individually may be insufficient, but taken as a whole, provide accurate, secure and accessible elections. […] The key to election security is in the people and policies that govern the use of voting equipment as much as it is in the design of each voting system. The review of any voting system must

take all those factors into consideration." (Sequoia Voting Systems, 2003). However, public concern was so great that Maryland's' Governor Ehrlich commissioned a special report by a national computer software company, SAIC, on the security of Diebold's system. The 200-page SAIC report confirmed numerous failings, including the lack of tampering and fraud protection and the lack of capacity for recount[1].

The third reason why computer scientists doubt the trustworthiness of electronic voting machines without paper backups is the fact that computerized voting gives the power to whoever controls the computer (Collier & Collier, 1992). Lynn Landers writes: "Only a few companies dominate the market for computer voting machines. Alarmingly, under U.S. federal law, no background checks are required on these companies or their employees. Felons and foreigners can, and do, own computer voting machine companies" (Landes, 2002). Computer scientists and journalists question the political affiliations of the leading voting companies. Harris found that just before the 1996 election Senator Chuck Hagel, a Nebraska Republican, used to run the voting company that provided most of the voting machines that count votes in his state. And he still owns a stake in the firm (Harris, 2003; Manjoo, 2003). Hagel failed to disclose his ties to the company whose machines counted his votes. When he was asked to describe every position he had held, paid or unpaid, he mentioned all sorts of jobs but not the fact that he had been the chairman of his own voting machine company. Harris points out: "This is not a grey area. This is lying" (Harris, 2003: 110). Conflicts of interest are seen everywhere. Ohio's largest daily newspaper, the Cleveland Plain Dealer reported that Walden O'Dell, the CEO of Diebold, is a major fundraiser of President Bush. Manjoo (2003a) notes: "In a letter to fellow Republicans, O'Dell said that he was 'committed to helping Ohio deliver its electoral votes to the president next year'. Even the people involved in the aforementioned Project P1583 who had to design the new standard for electronic voting machines were not beyond suspicion. It was implied that the committee leadership of Project P1583 is largely controlled by representatives of electronic voting machine vendor companies and others with vested interests. The problem is that when counties, states or countries consider purchasing electronic machines they usually base their choice of machine solely on the information from the vendors (Manjoo, 2003c). The opinion of unbiased technologists with no stakes in the voting system companies is often not taken into account and the decisions are made by people who don't understand the issues and don't understand much about how computer programs work.

As a result of the growing concern over the inadequacies of election equipment, a coalition of technical, legal and political experts have mobilised in November 2003 to put together a resolution calling for voter-verifiable e-voting across the EU (Kitcat, 2003).

[1] http://www.truevotemd.org/

3. Security in the TruE-Vote system

The TruE-Vote system is designed to realise an Internet based voting service. The EU project TruE-Vote aimed to contribute to the technological development and the increase of the community users' trust in information society technology tools to offer services, such as voting, by experimenting the potential of secure electronic voting integrated in the framework of a public key infrastructure. The objective of the project was to design and implement a secure Internet based voting system integrated with existing Public Key Infrastructures (PKI) and to demonstrate the advantages and the possibilities offered by secure electronic voting by means of voting sessions organized for Internet enabled users (community networks) and traditional users. The sociological analysis of the voting session results allowed us to understand the level of confidence and trust of the users ICT tools, the degree of acceptance of such tools in different socio-cultural areas and with respect to different users' technological skills, but also the media effects of the voting technology.

In a large number of field studies the use and effects of Internet voting were investigated. The field studies took place in five different locations: in three local situations (Newham, a neighbourhood in London; Orsay, a small town in France; CGIL, the Milanese department of an Italian trade union) and in two virtual communities (RCM - Rete Civica de Milano and OYK, a rural community network in Finland[2]). Due to legal constraints, the system could not be tested in national elections. Nevertheless, in all test sites, two or three real voting events were organized by e.g., the local authorities, or the trade union board, about official issues. For our analysis, we combined several methods and tools like questionnaires, direct observation, log files, voter interviews, analyses of the ballots and interviews with the ballot organizers. In this paper we will use the questionnaire data from 276 internet enabled users from the participating community networks RCM and OYK[3]. RCM (Rete Civica di Milano), is an urban community network in Milan and OYK (Learning Upper North Karelia)[4], is a rural community network in the eastern periphery of Finland, consisting of three neighbouring municipalities with a total area of 4500 km^2 km and a population of about 20,000 inhabitants.

During the design phase of the TruE-Vote system the project team had a lot of discussions about the verifiability of the vote. Although at the time we did not know of any other electronic voting systems that provided a voter-verifiable paper trail, we decided that in order to gain the trust of the users it would be wise to implement this requirement into the new system. Unfortunately, due to delays that are so common in large scale projects, the technicians were not able to realize the voter-verifiable audit trail for the pilots. The only form

[2] For a description of the demonstrators see Oostveen & Van den Besselaar (2002), *The implications of Internet voting on elections and civic participation.* Euricom Colloquium 2002.
[3] We will report about the results of the three local communities Newham, Orsay and CGIL on another occassion.

of verifiability provided took place within the system itself. The voter ticks the box of his choice, but the vote is not actually cast until it is confirmed. When "Confirm" is selected, the system will display all the operations required to actually cast the vote.

The voting application performs additional operations and controls before sending the vote to the ballot box to guarantee the voter's anonymity and the vote secrecy. The Voting Application connects to the 'Validator' for the vote validation and then to the 'Forwarder' to cast the vote. The 'Authenticator' receives the vote messages and decrypts them. After the Authenticator publishes the results, all the application modules send some information to a Trusted Third Party (TTP) in order to allow it to verify the systems integrity. The TTP verified that only valid voters submitted a vote and that the number of identifiers is at least equal to the number of votes cast. The Authenticator can also send to the TTP all the vote messages received from the Forwarder and a decrypted version of them. This way the digital signatures on each vote may be verified and the final tally recomputed to make sure that only legitimate votes were taken into consideration and the published tally is correct (Lanzi et al., 2003).

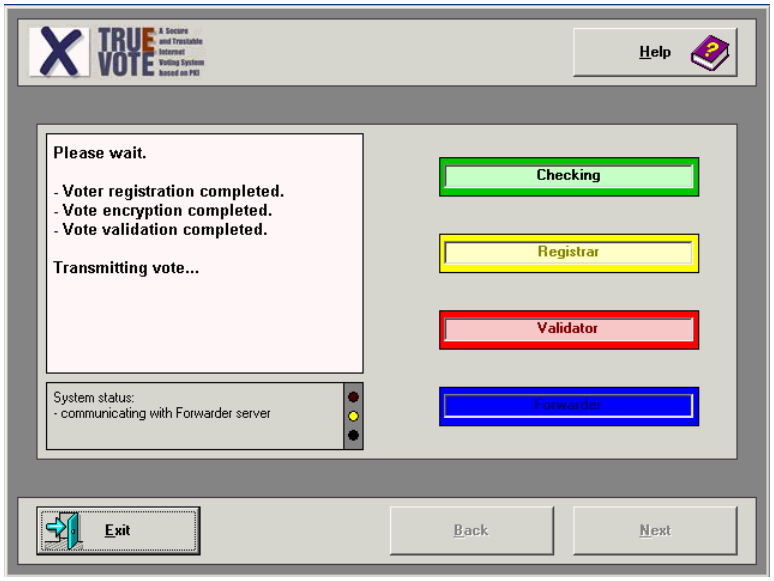

Figure 1 Screenshot of the TruE-Vote system

As described above, all of the verification takes place in the black box of the system. The users have no way of telling whether their votes were really cast the way they wanted them to be cast. The only thing that the system provides after the user has entered a vote into the computer is a screen which offers a digital representation of the vote. The TruE-Vote system then asks the voter to confirm the choice they have made. However, you cannot see your vote actually being recorded. As Harris puts it: "Asking you to 'verify' your vote by saying yes to a computer screen is exactly the same, in terms of data integrity, as asking you

[4] The Finnish name of the community network is Oppiva Ylä-Karjala (OYK)

to tell an election official your vote, which she then asks you to repeat while never letting you see what she wrote down. That procedure is absurd and would be trusted by no one" (Harris, 2003: 60). So, in the end a paper trail was not offered by the system. However, the questionnaires that were to be distributed among the people participating in the field studies were already designed based on the idea that the system would also have a voter-verifiable paper trail. Since the field studies took place in different countries, the English questionnaires had to be translated into Finnish, French and Italian. Time constraints made it impossible to change the questionnaires at the last moment and therefore the respondents were asked to respond to three statements about the verifiability of the system:

1. I could easily check that my vote has been counted.
2. It is difficult to verify the vote.
3. It is quick to verify the vote.

The answers were measured on a six-point scale, ranging from "Strongly Agree" to "Strongly Disagree". The three questions that were asked about verifiability were answered consistently.

We were amazed to find that the majority of the respondents agreed mildly to strongly that it was easy for them to check that their votes had been counted (61 per cent), while in fact the system does not provide this functionality. Only 5.8 percent disagreed strongly with this statement. In table 1 we present an overview of the opinions of the respondents related to their location, gender, trust in security and trust in new technologies.

Table 1: I could easily check that my vote had been counted

	Location		Sex		Trust in Security*		Trust in New Technology*		Total
%	RCM	OYK	Male	Female	No trust	trust	No trust	Trust	
Strongly Agree	17.6	9.2	16	11.5	7.8	17.8	11.6	15.3	14.6
Agree	22.2	20.4	18.2	28.7	15.6	24.4	23.2	21.3	21.5
Mildly Agree	24.4	25.5	23.5	27.6	23.3	25.6	24.6	24.8	24.8
Mildly Disagree	15.3	29.6	21.4	18.4	30.0	15.6	14.5	22.3	20.4
Disagree	14.2	9.2	13.9	9.2	12.2	12.8	17.4	10.9	12.4
Strongly Disagree	6.3	5.1	7.0	3.4	11.1	3.3	8.7	5.0	5.8
Total (N)	176	98	187	87	90	180	69	202	274

* Dichotomized variables

The other two statements about the verifiability of the system showed similar results. Sixty-eight per cent of the respondents disagreed mildly to strongly with the statement that it was difficult to verify their vote. In other words, they found it easy to verify their vote. Only 5.2 percent agreed strongly that it was difficult to verify their vote. Finally, in answer to the question whether it was quick to verify the vote 68 percent of the respondents said yes. Only 4.9 percent disagreed strongly. The next step was to test for correlations between a constructed variable named the "verifiability" variable, in which we combined the three verifiability questions. We created this new variable by taking the mean of the scores on the

three items. This variable measures the perceived level of verifiability of the TruE-Vote system. The neutral value is 3,5 with 1 and 6 as very much trust in verifiability and no trust at all, respectively. The average is 2.9, indicating a moderate trust, and the distribution is almost normal. We were surprised that the respondents were positive about the possibility to verify their vote and wanted to find out whether this opinion is related to background variables (for this we compare means using Anova) or context variables (Pearson correlations). We related the verifiability with other variables such as country, gender, usability, computer use, opinions about ICT, etc. Table 2 will summarize the results.

Using ANOVA we found that there is no relation between the place of voting and the users' opinion on the verifiability of the system. Whether respondents voted from home, work, school or a kiosk, they all gave similar answers to the three questions about the count of the vote. All of them were equally positive about the ease and speed of the verifying procedure.

Secondly, we found that there is a correlation with the variable gender. There were differences between the answers from men and women. The women seemed to agree slightly more with the statements than the men, but the differences weren't very large. This corresponds with women's overall higher trust in the security of the system. From previous analysis of our data (which we have reported in a paper on e-democracy, trust and social identity), we found that the participants from the community networks have less trust in the privacy of the system than in the security (Oostveen & van den Besselaar, 2003). We had measured both aspects of trust on a six-point scale and it was interesting to see that the respondents were in average moderately positive about the security of the systems, but negative about the privacy of the systems. What this means is that the respondents do not really fear attacks from hackers or from within, but they are concerned about their personal data. When people signed up for the field experiments, they had to provide a large amount of personalized data to be put on the smart cards for identification purposes. From their answers to the questionnaires and from the e-mails they have sent us, it became clear that they worried that their personal data would be used for other purposes, or that their data would be linked to their vote. Women seemed to have a slightly higher trust in the security and in the privacy protection of the systems than men did. Almost no difference existed between very frequent ICT users and the others.

There is also a correlation between the location (country) of the respondents and their trust in the verifiability of the system. We see that the respondents from Italy have a lower trust in the verifiability of the system than the Finnish respondents.

Using Pearson correlations we found no indication that the level of computer skills and experience influenced the opinion on the verifiability of the TruE-Vote system. We find it very surprising that there is no relation between the computer use of the respondents and their

opinion on the verifiability of the system. We would have expected that frequent computer users would have been far more critical about the security and verifiability of the system. We also expected that users with little computer experience would think that the system is verifiable but that it is their lack of knowledge which makes that they can't see it. However, people who use the computer and the internet more frequent seem to judge the verifiability of the system in the same way as people who use the computer less. Also, users who judged themselves to be very expert with computers had the same opinion as people who saw themselves as hardly computer savvy.

People with a low trust in the security of TruE-Vote show that they are more concerned about the verifiability of the voting system than the people who do trust the security. This is what you would expect. We find the same for trust in new technology. People with a lower trust in new technologies believe less in the ability to audit the election for verifiability. For trust in privacy we did not find a correlation with the variable of verifiability. Users who feel that new ICT's can not be avoided in the future have more trust in the verifiability of the system.

The last variables we look at are those related to the usability of the system. We see that there is a relation between the usability and the opinion about verifiability (Pearson 0.531). People who find the TruE-Vote system easy to use (fast, easy to install, easy to connect, easy to correct mistakes, etc) also trust the verifiability more than people who rated the usability more negatively.

Summing up, we can say that the more careless voters are about the security of ICT based systems, and the more they believe that the TruE-Vote system is secure, the more they also believe that the TruE-Vote system is verifiable. The same holds for the belief that new voting technologies are a form of progress, the opinion that increasing use of ICT is unavoidable, and the general opinion about the usability of the TruE-Vote system. Finally, the opinion about voting in general has some effect: the stronger one finds voting a public duty, the better one evaluates the verifiability of the system.

verifiability of	average	sign	N
men / women	3.05 / 2,71	0.034	188 / 88
Italia / Finland	3.03 / 2.77	0.09	177 / 99
verifiability by	correlation	sign	N
trust in security	0.323	0.000	275
trust in new voting technology	0.181	0.003	273
voting is public duty	0.132	0.029	273
careless about privacy	0.128	0.034	272

Table 2: Trust in verifiability

So what do these results tell us? We have a system that does not really show people that their votes are properly counted. Everything happens within the machine and is not visible for the users, but this does not seem to bother them too much. What is it that they actually trust? Is it the system? Or is it the authority of the organizers? The majority of the respondents say that they could easily check that their vote was counted. They said it was easy and quick to do this. Therefore, we have to conclude that their opinion is more based on *perception* than on facts. Does this mean that it is not important how secure a system is, as long as people trust it to be secure? Does this mean that as long as we tell the users a bunch of lies about the security, privacy or verifiability of the system they will believe it and act accordingly?

From the data we see that the trust of the users in relation to the verifiability of the system is related to the system itself, as well as to things that have nothing to do with the technology. On the technology side of the system we saw that the trust in the security and the usability of the system plays a large role. People do base part of their opinion on these issues. The more people trust in the security and the better the usability of the system, the less they will doubt about the ability to verify the count of the vote. From this we learn that improving the security and the usability will have an impact on gaining or restoring pubic confidence and trust in electronic voting systems.

However, a lot of the variables that correlate with the trust in verifiability have nothing to do with the technology itself, but more with the social context in which the new technology is embedded. We saw that both the location and the gender of the participants play a role. Also their trust in new technologies and the unavoidability of ICT's influences their opinion. Users with a more positive view on technology will be more willing to believe that the system is verifiable, even if this is not really the case. We have seen in this paper that people will use insecure systems or black box technologies if they think of them as being secure. But how do people form their opinion about the security and privacy of new technologies and existing ICT's? First of all, we think that the reputation and professionalism of the organizing institution might have an influence on the perception of people. If a local or national government is fully trusted by citizens then they are more likely to also trust the security of the system. This might also explain the differences in opinion we saw between the Finnish and the Italian respondents. Secondly, we think that the attitude of the mass media also influences the opinion of the users. When newspapers or TV programs cover negative stories about certain technologies (rightfully or not), then people will be influenced by this accordingly. Thirdly, the views of friends, family and colleagues play an important part in forming an opinion. Finally, one could assume that the convenience which a new technology might bring people will also influence their opinion about it. In the Technology Acceptance

Model (TAM) which was developed by Davis (1989) to explain IT acceptance, two technology acceptance measures were introduced – usefulness and ease of use. The model focuses on individual users' beliefs, attitudes, and behavioural intentions towards technology use. *Perceived usefulness* is defined as 'the degree to which a person believes that using a particular system would enhance his or her job performance'. *Perceived ease of use* was defined by Davis as 'the degree to which a person believes that using a particular system would be free from effort'. It is this last measure on which we focus here. Earlier research on the adoption of innovations suggested a prominent role for perceived ease of use (Tornatzky and Klein, 1982). We will take the mobile phone as an example of the argument that ease of use and the subsequent convenience might influence peoples' beliefs and attitudes towards using new technologies. Ever since people started using mobile phones the issue of electromagnetic field (EMF) radiation from cell phones has been controversial. Most experts believe that it is insignificant. However, there is a significant body of evidence to suggest that cell phone radiation can indeed cause health problems. For instance, one study published in the European Journal of Cancer Prevention, looked at 1,617 Swedish patients diagnosed with brain tumours and found that those who had used Nordic Mobile Telephone handsets (the first generation cell phones) had a 30 per cent higher risk of developing brain tumours than people who had not used that type of phone, particularly on the side of the brain used during calls. For those using the phones for more than 10 years, the risk was 80 per cent greater (Hardell et al, 2002). Other studies however did not find a connection between mobile phones and cancer. Hansson Mild, professor at the National Institute for Working Life states that nothing can be really said yet about the currently widely used digital Global System for Mobile Communications phones (GSM). "These are tumours that develop very slowly, and GSM does not have users who have been using it for 10 years" (Rense, 2002). The debate about the risk of mobile phones for the health of the users is still ongoing (Hardell et al, 2003), and users get very mixed information about the risks of mobile phones. Nonetheless, the majority of people decided to trust the safety of the phones and use them despite the concerns because they are easy to use and bring them so much convenience. From this it is obvious that users of technology pay more attention to first-order effects than to second-order effects. Second-order effects are the unintended consequences of a technology which often have a more powerful impact on society than the more obvious first-order changes (Cooper, 2001). It is likely that if citizens see electronic voting as an easy and convenient way to cast their votes in the future, they might be less concerned about its security issues. This could of course also work the other way around. A system could be one hundred percent safe and secure, but if users don't trust it they will not use it.

4. Conclusions

This paper dealt with the social issues of IT security, focusing on e-voting systems in particular. With current (paper-based) voting systems, errors are likely to be on a relative small scale. Electronic voting, on the other hand, substantially increases the scale of potential problems. This has its impact on public confidence. The complex technical questions with regard to security and other issues of electronic voting systems should be answered before these systems are to be used at parliamentary and other governmental elections on any level. At the moment the topic of voter-verifiability is very much in the limelight. In order to guarantee a true democracy it is important to have as secure a voting system as possible. Requiring a voter-verifiable paper trail is, as we have seen, one important step in that direction.

Many technologists think that the solutions for security and trust issues lie in adjusting and improving the technology. David Dill is one of these people who think technology is the answer. He says: “Instead of trying to convince people the machines are safe, the industry should fix the technology and restore public confidence by making the voting process transparent, improving certification standards for the equipment and (ensuring) there is some way to do a recount if there is a question about an election" (Zetter, 2003). But is this the best solution? Will users trust the system more when it is more secure? Will offering voter-verifiable paper trails work to gain trust from people or are there other non-technological issues that are of equal or more importance? Some well-known technologists like Whitfield Diffie, Phil Zimmermann, Neal Stephenson, all known for their work on cryptography and Tim Berners-Lee, creator of the World Wide Web, start to acknowledge the limitations of a techno centric approach to the complicated questions of privacy, security and freedom. They are moving towards recognition of social and political realities. True techno-believers are sure that they can guarantee the privacy and security of people with physics and mathematics. But after thirty years of working on perfecting cryptography some of the techno-believers are changing their views on privacy and security issues. Stephenson, for instance, says that “the best defense for one’s privacy and personal integrity turns out to be not cryptography but ‘social structures’” (Ullman, 2000). He furthermore states that without a sociopolitical context, cryptography is not going to protect you. Zimmermann, creator of PGP (Pretty Good Privacy) encryption, admits that code is not enough and that he never intended encryption, by itself, to work. Whitfield Diffie, together with Martin Hellman the discoverer of public-key encryption, has always supported the view that technology would protect the individual from the reach of government. However, in a speech held at the 10th Computers, Freedom and Privacy Conference (Toronto, 2000) Diffie states that at the beginning of his career he had a very mathematical and very inapplicable idea about authentication (Ullman,

2000). He was sure that crypto was a security technique that didn't require trusting anyone else. But now that he is older he says that it turns out you have to trust other people. It is a rejection of the ideal of trust in physics and mathematics. As Ullman says: "Like Stephenson, like the reluctant Zimmermann, like the unhappy Berners-Lee, the father of public key encryption has come to the conclusion that software may reduce the amount of trust you need in human beings, but as one moves about in the world, the sense of security, privacy and autonomy turns out to be "a function of social structures".

From our research within the TruE-Vote project we have indeed seen how important the social context is for the trust people have in a system. People should not just have to trust in the integrity of a voting system or the people who designed, developed and implemented it. With a system so crucial to the existence of our democracy trust in technology alone is not sufficient. In order to fully understand citizens' willingness to use electronic voting systems we need to look as much into the sociopolitical issues as into the technological issues. Both need to be taken into account to make electronic voting a secure and successful new voting method. The entire context of elections has an impact on the trust and perception of citizens with respect to security. A crucial question to be answered in future research is *under which conditions* the opportunities and risks of electronic voting will materialize, and how deliberate policies of relevant actors may influence these conditions. This may be related to the 'objective quality' of the systems, conditions in the environment, the level of trust in the system, and the mutual relations between these three factors.

5. Acknowledgements

The authors gratefully acknowledge funding from the TruE-Vote project (IST-2000-29424). We are grateful to our partners for their contributions to the work reported here: Postecom (Coordinator – Italy), Abacus (Italy), Certinomis (France), CGIL (Italy), Glocal (Finland), Newham (UK), NIWI-KNAW (Netherlands), Orsay (France), RCM (Italy), Smile (Italy), and University of Milano (Italy). Part of the work was done in the former Social Informatics group at the University of Amsterdam.

6. References

Coleman, S. et al**.** (2002) Elections in the 21st Century: from paper ballot to e-voting. The Independent Commission on Alternative Voting Methods. London: Electoral Reform Society.

Collier, J., Collier, K. (1992) VoteScam: The Stealing of America. Victoria House Press.

Cooper, A. (2001) The second-order effects of wireless. Newsletter Cooper Interaction Design. Online: http://www.cooper.com

Diebold Election Systems (2003) Checks and Balances in elections equipment and procedures prevent alleged fraud scenarios.

Davis, F.D. (1989) Perceived Usefulness, Perceived ease of Use, and User acceptance of Information Technology. MIS Quarterly, 13 (3), 319-340.

Hardell, L., Hallquist, A., Hansson, K., Mild, K.H., Carlberg, M., Phlson, A., Lilja, A. (2002) Cellular and cordless telephones and the risk for brain tumours. European Journal of Cancer Prevention v.11, n.4, August 2002.

Hardell L, Mild KH, Carlberg M. (2003) Further aspects on cellular and cordless telephones and brain tumours. International Journal of Oncology February 2003; 22(2):399-407.

Harris, B. (2003) Black Box Voting: Vote Tampering in the 21st Century. Elon House/Plan Nine, July 2003.

Internet Policy Institute (2001) Report of the National Workshop on Internet Voting: Issues and Research Agenda. March 2001.

Kitcat, J. (2003) FIPR Foundation for Information Policy Research. New campaign calls for safe e-voting. Online: http://www.fipr.org/press/031104vote.html

Kohno, T., Stubbefield, A. Rubin, A., Wallach, D. (2003) Analysis of an Electronic Voting System. John Hopkins Information Security Institute technical Report TR-2003-19, July 23, 2003.

Konrad, R. (2003) E-voting critics point to security hole. California primary results appeared online before polls closed. Associated Press MSNBC News. Online: http://stacks.msnbc.com/news/964736.asp?0dm=n15ot

Landes, L. (2002) Elections in America – Assume Crooks Are In Control. Online: http://www.commondreams.org/views02/0916-04.htm

Lanzi, A., Martignoni, L., Masiero, S., Poletti, G., Rosti, E. (2003) TruE-Vote Architectural Design. Deliverable 3.1. IST-2000-29424D.

Levy, S. (1994) Prophet of Privacy. Wired Magazine. Online: http://www.wired.com/wired/archive/2.11/diffie_pr.html

Manjoo, F. (2003) Hacking democracy? Online: http://www.salon.com/tech/feature/2003/02/20/voting_machines/print.html

Manjoo, F. (2003b) Another case of electronic vote-tampering? Online: http://www.salon.com/tech/feature/2003/09/29/voting_machine_standards

Manjoo, F. (2003c) An open invitation to election fraud. Online: http://www.salon.com/tech/feature/2003/09/23/bev_harris

McGaley, M., Gibson, J.P. (2003) Electronic Voting: A Safety Critical System.

Mercuri, R. (2001) Dr. Rebecca Mercuri's Statement on Electronic Voting. Online: http://www.notablesoftware.com/RMstatement.html

Oostveen, A., Van den Besselaar (2004) E-democracy, Trust and Social Identity: Experiments with E-voting technologies. Forthcoming.

Rense, J. (2002) Some Early Cellphones Pose Increased Brain Tumor Risk. Online: http://www.rense.com/general28/cisire.htm

Rubin, A. (2003) Response to Diebold's Technical Analysis. Online: http://avirubin.com/vote/response.html

Sequoia Voting Systems (2003) Sequoia Discusses Safeguards of Electronic Voting. Online: http://www.sequoiavote.com/article.php?id=50

Tornatzky, L.G., Klein, R.J. (1982) Innovation characteristics and Innovation adoption-implementation: a meta-analysis of findings. IEEE transactions on Engineering Management, EM 29, 28-45.

Ullman, E. (2000) Twilight of the crypto-geeks. Online: http://www.salon.com/tech/feature/2000/04/13/libertarians

Zetter, K. (2003) E-Vote Firms Seek Voter Approval . Wired News. Online: http://www.wired.com/news/evote/0,2645,60864,00.html