# Security as belief
# User's perceptions on the security of electronic voting systems

Anne-Marie Oostveen, Peter van den Besselaar

Department of Social Sciences, NIWI- KNAW
Royal Netherlands Academy of Arts and Sciences, The NETHERLANDS
{Anne-Marie.Oostveen | Peter.Van.den.Besselaar}@niwi.knaw.nl

**Abstract** In this paper a pilot e-voting system is being studied 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. According to many researchers a voter-verified paper trail is the only way voters can have confidence that their vote has been recorded correctly. However, technologists start to acknowledge that security mechanisms are fundamental social mechanisms. Trust is of great importance; people no longer have a blind faith in scientific objectivity and the "experts". We examine the opinions of users involved in the testing of the TruE-Vote e-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 favor of electronic voting. They see a lot of possibilities in this new technology. Most proponents argue that the adoption of e-voting systems would increase voter participation. 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, quickest and most efficient way to administer elections and count votes. However, the cost of online voting would vary enormously depending on the type of system employed and the type of security used [Co]. But from the first trials with e-voting, 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 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 [Co].

Broadly speaking, each election involves four distinct stages: registration, validation, casting of the vote and tallying. Each of the stages can take place by using physical or electronic procedures. Computer-based voting systems need to satisfy a number of criteria like eligibility, uniqueness, accuracy, reliability, verifiability, secrecy, etc. to guarantee a democratic election which is free, equal and secret [IPI]. In this paper we focus on the criterion of verifiability. Public confidence in the election process depends on the verifiability 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. Electronic voting is likely to lead to changes in how the public maintains confidence in the integrity of elections. With e-voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process [IPI]. Media stories about 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 or passwords, encryption, digital signature, smart cards or biometric identifiers. It is important to make the voting and counting processes as transparent as possible. 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 way to provide a voter-verified audit trial (VVAT) 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." [Me]

Unfortunately, most of the e-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. These errors came to light by accident when voters' rolls were compared with voter tallies and the numbers didn't add up. 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" [Ha]. 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 VVATs) 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 VVAT will improve the trust of people in e-voting systems, but history has shown us that trust in a new technology alone 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 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 they 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 sociopolitical 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” [Ul]. 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

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 correct than they will never accept that those votes represent their voice. It is therefore that computer scientists, social researchers and engineers are promoting a hybrid system. They favor 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. These changes may not be detected because of the secrecy of the vote. 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 VVAT which provides a permanent record of each vote. This way the voter can check to ensure that it represents their intent. 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. When there is any doubt about the results of the election, there is the possibility of a manual recount.

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 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 [Ma2]. Even more problematic, the standard failed to require or even recommend that voting machines be truly 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 the 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.” [Ma2].

A second reason why more scientists started to worry about electronic voting systems without VVAT was the uproar about the Diebold voting system. Numerous reports have found Diebold machines and other computer voting systems vulnerable to error and tampering [KS; Ha; Ko; Ma1; Ma3]. 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” [Ha]. 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” [Ha]. But lo and behold! More or less by mistake Diebold published the source code on a public internet site. Harris discovered that Diebold’s voting software is so flawed that anyone with access to the system’s computer can change the votes and overwrite the audit trail without leaving any record [Ma3]. But someone could also get into the system by hacking the telephone system or by going backwards in through the Internet [Ma3]. 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. Scientists at the Johns Hopkins University also found that the security in Diebold’s software was “far below even the most minimal security standards applicable in other contexts”. Their report shows that insiders as well as outsiders can do the damage [KS]. In reaction to the security issues identified by computer scientists, Diebold claims that the Johns Hopkins team is not familiar with the election processes, makes false technical assumptions, has an inadequate research methodology and makes insufficient use of input from election experts [Di; KS]. The voting machine vendors furthermore state that researchers should have reviewed all the different layers of security in voting systems together. Sequoia Voting Systems [SV] 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 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 [CC]. 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.” [La] Computer scientists and journalists question the political affiliations of the leading voting companies. Harris found that just before the 1996 election Senator 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 owned a stake in the firm [Ha; Ma1]. Hagel failed to disclose his ties to the company whose machines counted his votes. Harris points out: “This is not a grey area. This is lying” [Ha]. Conflicts of interest are seen everywhere. Ohio’s newspaper, the Cleveland Plain Dealer reported that O’Dell, the CEO of Diebold, is a major fundraiser of President Bush. Manjoo [Ma1] 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 is largely controlled by representatives of e-voting machine vendor companies and others with vested interests. The problem is that when counties, states or countries consider purchasing electronic voting machines they usually base their choice of machine solely on the information from the vendors [Ma3]. 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.

## 3. Case Study: Security in the TruE-Vote system

The objective of the TruE-Vote project was to design and implement a secure Internet based voting system integrated with existing Public Key Infrastructures, and to demonstrate the possibilities of e-voting and e-polling by means of voting and polling experiments with Internet enabled users (members of 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 in the technology, the relation between socio-cultural background and technological skills of the users and the level of acceptance of e-voting technology, and finally the effects of e-voting technology on voting behavior.

We conducted fourteen field studies 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 community networks (RCM in Milan and OYK in rural Finland). 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 the local authorities or the trade union board about policy issues. For our study, we combined several methods and tools like questionnaires, direct observation, log files, analyses of the ballots and interviews with voters and ballot organizers. This paper uses the data from the internet enabled users at RCM and OYK.

During the design phase of the TruE-Vote system the project team had many discussions about the verifiability of the vote. Although at the time we did not know of any other electronic voting systems that provided a VVAT, we decided that 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 VVAT in time for the pilots. The only form 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. Since 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 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 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” [Ha]. So, in the end a paper trail was not offered by the system. However, the questionnaires that were to be distributed among the participants were already designed based on the idea that the system would 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 them 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.

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 percent), while in fact the system does not provide this functionality. Only 5.8 percent disagreed strongly with this statement. The other two statements about the verifiability of the system showed similar results. 68 percent 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, and 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 as very much trust in verifiability and 6 as and no trust at all, respectively. The average is 2.9, indicating a moderate trust. 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 personal characteristics (gender, age, computer literacy, opinion about usability of TrueVote and about ICT in general) or to context variables (place of voting, country).

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. On the other hand, the *country* matters: we found that the respondents from Italy have a lower trust in the verifiability of the system than the Finnish respondents.

The level of *computer skills and experience* does not correlate with the opinion on the verifiability of the TruE-Vote system. We find this very surprising, as we 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, as they lack the knowledge which makes them understand what really happened. 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. We did not find any correlation with the age of the respondents.

*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 we found that the users hardly *trust the privacy* of the system, but do have reasonable *trust in the security* [OV]. What this means is that the respondents do not really fear fraud or attacks from hackers, 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 both the security and the privacy protection of the systems than men did. Users with a low trust in the security of True-Vote are also 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 in general*. People with a lower trust in new technologies believe less in the verifiability of electronic ballots. On the other hand, trust in privacy does not correlate with verifiability. Users who feel that new *ICT's can not be avoided* in the future have more trust in the verifiability of the system. Finally, there is a relation between the opinion about the usability and the opinion about verifiability (r = 0.545). 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.

| **verifiability** | **Mean (ANOVA)** | **Sign** | **N** |
|---|---|---|---|
| men / women | 3.05 / 2,71 | 0.034 | 188 / 88 |
| Italy / Finland | 3.03 / 2.77 | 0.09 | 177 / 99 |
| **verifiability by** | **Correlation (r)** | **Sign** | **N** |
| trust in security | 0.32 | 0.000 | 272 |
| trust in new voting technology | 0.18 | 0.003 | 273 |
| voting is public duty | 0.12 | 0.048 | 273 |
| unconcerned about privacy | 0.13 | 0.034 | 272 |
| unavoidability of ICT | 0.24 | 0.000 | 274 |
| usability | 0.55 | 0.000 | 276 |

*Table 1: Trust in verifiability by other variables*

Summing up, we can say that the less concerned people are about the security of ICT in general, 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 indicate progress, the opinion that increasing use of ICT is unavoidable, and the opinion about the general 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. So what do we learn from these findings? We have a system that does not 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. Thus, 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?

Our data show that the trust of users in relation to the verifiability of a system is not only related to the system itself, but also 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 public confidence and trust in e-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 trust in new technologies and the unavoidability of ICT's influences user's opinion. Users with a positive view on technology are more inclined to believe that the system is verifiable, even if this is not 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? Further research is needed to investigate which non-technical factors influence trust and the acceptance of new technology. First of all, we think that the reputation and professionalism of the organizing institution might have be a factor that influences 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 explain the differences in opinion we saw between the Finnish and Italian respondents. Secondly, we think that the attitude of the mass media influences the opinion of the users. When newspapers or TV programs cover negative stories about certain technologies (rightfully or not), people will be influenced by this accordingly. Thirdly, the views of friends, family and colleagues may play an important part in forming an opinion. Finally, one could assume that the convenience that a new technology might bring people will influence their opinion about it. We will take the mobile phone as an example of this argument. Ever since people started using mobile phones the issue of electromagnetic field 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 [HH; Re]. The debate about the risk of mobile phones for the health of the users is still ongoing and users receive 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 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. Therefore it is likely that if citizens see e-voting as a convenient way to cast their votes, they might be less concerned about its security issues. This could 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

With current 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 e-voting systems should be answered before the systems are to be used at 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 VVAT 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. Dill 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" [Ze]. 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 Diffie, Zimmermann, Stephenson, all known for their work on cryptography and 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 and admit that you have to trust ‘social structures’. It is a rejection of the ideal of trust in physics and mathematics [Ul].

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.

## 5. Acknowledgements

The TruE-Vote project (IST-2000-29424) was partly funded by the European Commission. We are grateful to our partners: Postecom, CGIL, Abacus, RCM, Smile, and the University of Milano (all Italy), Certinomis, Orsay (both France), Glocal (Finland), Newham (UK), NIWI-KNAW (Netherlands). Part of the work was done in the former Social Informatics group at the University of Amsterdam. We would like to thank Vanessa Dirksen and Bruce Clark for their comments.

## References

[Co] 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 Soc.

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

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

[HH] 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, Aug02.

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

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

[KS] Kohno, T., Stubbefield, A. Rubin, A., Wallach, D. (2003) Analysis of an Electronic Voting System. Johns Hopkins Information Security Institute technical Report TR-2003-19.

[Ko] 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

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

[Ma1] Manjoo, F. (2003) Hacking democracy?
Online: http://www.salon.com/tech/feature/2003/02/20/voting_machines/print.html

[Ma2] Manjoo, F. (2003b) Another case of electronic vote-tampering?
Online: http://www.salon.com/tech/feature/2003/09/29/voting_machine_standards

[Ma3] Manjoo, F. (2003c) An open invitation to election fraud. Online:
http://www.salon.com/tech/feature/2003/09/23/bev_harris

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

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

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

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

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

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

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