Non-Technical Risks of Remote Electronic Voting

Anne-Marie Oostveen
Rathenau Institute, The Netherlands

Peter van den Besselaar
Rathenau Institute, The Netherlands and Universiteit van Amsterdam, The Netherlands

INTRODUCTION

A few years ago, remote electronic voting seemed like a good idea for the near future. Globally, voting turnout figures are dropping dramatically (Electoral Commission, 2002) and politicians are therefore trying to find ways to increase civic participation. One solution is to make the voting process more convenient by giving voters the opportunity to submit their governmental election ballots over the Internet from home or work, or through their mobile phones using SMS. In this way, people will not have to leave the comfort of their homes or their work routines to have their voices heard. What a great boost this would be for our Western democracy! Citizens who live overseas, housebound people, or business travellers, everybody could use a computer to cast a ballot online. However, we will argue in this article that for several reasons remote electronic voting does pose a real challenge for e-government and might not necessarily be the best way forward.

BACKGROUND

Many politicians and legislators are in favour of this new voting technology. They expect it will bring convenience to the voters, may increase turnout among the young, may result in cheap, efficient vote counting, and may reduce the incidence of human error (Dictson & Ray, 2000; Mohen & Glidden, 2001). Technological development of electronic voting is stimulated by national governments, and also in the context of the European Union (EU) Framework Programs.[1] On the other hand, opponents of Internet voting claim that besides large security risks, and the lack of equal access to the Internet for all citizens, it is not the voting *method* that matters. Low turnout is perceived as a symptom of a deepening crisis of democracy. Widespread indifference to, and ignorance of politics, is causing an evaporation of the concepts of citizenship and participation (Eliasoph, 1998). Previous reforms to make voting more convenient have had little effect on turnout levels and virtually none on the composition of the electorate (Internet Policy Institute, 2001). In our own research in which we examined a series of experiments with e-voting and e-polling, we did not see any positive influence on voting turnout. In four different sites a series of three e-polls took place, and in each case, we saw a declining turnout, suggesting that the effect of new technology on turnout is at best only temporary (Van den Besselaar, Oostveen, De Cindio, & Ferrazzi, 2003).

Nevertheless, even without affecting voting turnout, e-voting and e-polling technologies are of great importance. In order to clarify the opportunities and risks for democratic processes, we studied some 15 experiments with an e-voting system. The conclusion is that "voting in your underwear" (Arent, 1999) does not seem a valid option—at least not at this moment. Various technical, organisational, and behavioural issues are at stake. We discuss the main issues here.[2] We focus mainly on remote e-voting, but several of the risks discussed are also relevant for e-voting in a polling station using a voting computer, and for other (nonelectronic) forms of remote voting, such as postal voting.

SECURITY AND VERIFIABILITY

Many people are concerned about the *security of remote voting* (Harris, 2003; McGaley & Gibson, 2003; Rubin, 2000). When people use computers from home or work, the machines are never as secure as the voting machines used in supervised kiosks or polling stations. Personal computers might be more vulnerable to hackers, denial of service attacks, viruses, or phantom Web sites which are used to divert voters (Kohno, Stubbefield, Rubin, & Wallach, 2003). Another problem with the use of personal computers at home or work is that the *requirement of verifiability* becomes very difficult to realize (Mercuri, 1993). Internet voting systems pose a problem in that the tallying process is not transparent. Voters should be able

to see that their votes are tabulated correctly. The best way to do this is to provide a voter-verifiable physical audit trail (Mercuri, 2001). If citizens do not trust that the elections they participate in are fair and that the votes are counted correctly, then they may not accept that the final votes represent their opinion. At polling stations the voting system could provide such a voter verifiable audit by printing a permanent paper record of each vote. In case of any doubts about the results of the election, there is then the possibility of a manual recount of these paper ballots (McGaley & Gibson, 2003). However, voting computers often do not have this facility, which makes recounting impossible—also in the polling station. If we switch from e-voting in the polling station to Internet voting from home, this becomes an even more serious problem: the paper trail is then impossible.

Yet, technical vulnerabilities are not the only threats to the security, integrity, and secrecy of Internet ballots. Social issues also play a very important role. Voting systems should guarantee a democratic election which is free, equal, transparent, and secret. However, *remote* e-voting cannot guarantee any of these criteria. This article will give an overview of five nontechnical reasons why we think (remote) e-voting poses a real challenge for e-governments around the world (Oostveen, 2006).

FREE AND SECRET VOTING

In a recommendation report written by the Council of Europe (2004), five basic principles of democratic elections and referenda are specified. Elections need to be universal, equal, free, secret, and there should be direct suffrage. These principles apply to traditional voting as well as to new voting methods. With e-voting the voters must be identified by the system; the tallier must be able to distinguish the votes cast by valid voters from those cast by voters who are noneligible. At the same time the votes must remain anonymous and secret. No one should be able to determine how any individual voted, and voters should not be able to prove how they voted because this would facilitate vote selling or coercion. Remote e-voting increases the risk of coercion of the voter by, for instance, a dominant spouse, the teacher at school, or the boss in the office.

Our research shows that the possibility of coercion is a real concern among voters (Oostveen & Van den Besselaar, 2004). We organised 12 focus groups and one online forum in four different countries with voters and organisers of ballots (pollsters). We ensured that there were vast differences in the socio-demographic makeup across the respondents in each of the focus groups, including age, gender, income, and ethnicity (further details in Oostveen & Van den Besselaar, 2004; Oostveen, 2006). The greatest risk of e-voting, according to the majority of the panellists, is the possibility that a voter can be forced by someone else to vote for a certain alternative. An Italian voter pointed out: "At first I thought it was a good idea, but now I fear the influence and pressure that family members could exert on voters." With remote voting there will never be the same privacy that a voting booth provides.

This phenomenon of "family voting" is also possible with other voting technologies. Husbands could accompany wives into the polling booth, and this indeed is also a real problem in many cases. However, appropriate regulation may prevent this from occurring, because voting in a polling station is in the public domain and therefore controllable. Postal voting makes coercive family voting also a possibility. As is often argued, the education of voters and a stable political situation may heavily reduce the risks of family voting. In our view, however, the voting system should be robust also in periods of political tension. Therefore, postal voting does not seem to be a good idea either.

Remote electronic radicalizes this problem. Our research shows that many voters do not trust that their privacy is guaranteed in e-voting systems. And these voters feel that surveillance may alter their voting behaviour, as our research indicates (Oostveen & Van den Besselaar, 2005). Here, there is a need for additional research and experimentation before deciding about the deployment of the new voting technology.

DIGITAL DIVIDE

E-voting has to deal with an existing digital divide, in which there is an upper-class bias (Alvarez & Nagler, 2000; Phillips & von Spakovsky, 2001). This digital divide can be expected to influence the participation in, and the outcome of, ballots. According to many observers the digital divide is declining, yet this is generally measured in terms of *access* to the Internet. However, divides may be much more subtle and related to skills required to install the software and hardware, learning, social networks that provide help, ownership of advanced versus older types of computers, insights into the security and risks, and so on. From the literature we learn that despite the narrowing of the "digital divide," Internet connections are still not distributed evenly across racial, gender, age, regional, and socioeconomic lines. This applies even more so for the skills needed to use the technology (Wellman & Haythornthwaite, 2002). Demographic groups with less access and less familiarity in using computers might find some types of e-voting difficult or intimidating. There-