International Working Group
on Data Protection
in Telecommunications

Working Paper on

Data Protection and Online Voting in Parliamentary and other Governmental Elections[1]

adopted at the 30th meeting of the Working Group on 28th August 2001 in Berlin

Modern communications technology, in particular the Internet, may have the potential to be used as an additional way of preparing or facilitating participation in elections on local, state or worldwide levels. “Online voting”, “electronic voting” and “e-democracy” are keywords in recent public discussions. In a number of countries the legal framework is being changed to allow for online voting. Universities and other bodies have held internal online elections for representative bodies of students.

Two forms of online voting can be distinguished:

- online voting with certified hard- and software at official polling stations (“closed” or “end-to-end”-systems);

- online voting from any input device (e.g. home PCs, mobile phones) with uncertified software (“open systems”).

The second option leads to a general problem of absentee voting since ballot secrecy is not ensured on the same level at one’s home or place of employment as in a polling booth.

Any technology used in this context has to meet the basic constitutional requirements for a democratic voting procedure. It is generally accepted that parliamentary and other governmental elections have to be free, equal and secret. At the same time the election procedure has to be transparent and subject to public scrutiny.

In the case of binding elections for parliaments and other representative political bodies the requirement of ballot secrecy is crucial. At the same time ballot secrecy will have to be reconciled with transparency and auditability of the entire voting procedure. The experience of surveillance and vote-rigging in non-democratic societies has underlined that the trustworthiness of any political system is at stake here. Whereas paper-ballot elections are transparent online voting procedures are not transparent to same extent. Online voting may be even more secure than conventional voting methods. However, voting not only has to be secure, it has to be seen to be secure. Cryptographic methods (e.g. blind signatures) and the informational separation of powers and functions (separation of privilege). between servers which check voter registration and which collect and count votes are un-

[1] The scope of this paper is restricted to elections for representative political bodies and public offices. The term “Governmental” includes all (i.e. the legislative, executive and judicial) branches of government.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

der discussion. They are highly complex but at the same time they will have to compensate for the lack of transparency. These proposals have to be scrutinised carefully and discussed in public. Since voter confidence is essential for the democratic process considerable caution is appropriate. The US Presidential Election 2000 put voting technology at the centre of intense public controversy. Public unease can arise if voting technology is not trusted or is perceived to frustrate the public's will in the voting, counting or checking processes.

The Working Group therefore makes the following recommendations:

- The complex technical questions with regard to dependability including security and availability of online voting systems (protection against unauthorized access and "denial of service"-attacks) should be answered before any such system is used at parliamentary and other governmental elections on any level; these systems should be subject to a thorough risk analysis and testing[2].

- Authentication procedures for voters in electronic ballots which are used before casting the vote in order to ascertain the right to vote, to prevent votes being cast more than once and at the same time to ensure ballot secrecy, should be no less secure than the procedures used in paper ballots.

- While the system should warn the voter if the vote has not been registered or transmitted correctly, receipt-free vote casting must be ensured in order to diminish the risk of influencing prospective voters or victimising those who have voted. No caching or electronic recording of the individual votes cast should be allowed after they have been counted.

- The entire hard- and software including the source-code has to be documented and open to scrutiny.

- Trusted certification procedures for hard- and software have to be implemented.

[2] Recent research in the U.S. suggests that it might take at least ten years before this goal is achieved; cf. the Report of the California Institute of Technology / Massachusetts Institute of Technology, Voting Technology Project, Voting – What Is – What Could Be, July 2001, <http://www.vote.caltech.edu/Reports/index.html>