Internet Voting and Individual Verifiability: The Norwegian Return Codes

Jordi Barrat i Esteve, Michel Chevallier, Ben Goldsmith, David Jandura, John Turner and Rakesh Sharma

Presentation Overview

- Explore the standard of secret voting
- Review secrecy and individual verification mechanisms in the Norwegian internet voting system
- Assess whether the return codes violate the secrecy of the vote in general
- Assess whether the return code is a voting receipt

Standard of Secret Voting

- Origin in the ICCPR, repeated in many subsequent treaties/political agreements
- CoE Recommendations on E-voting
  - Section on secrecy (16-19)
  - Section on freedom of the vote (9-15)
  - Technical and operational standards (34,35,51,93)
  - Secrecy and freedom of the vote vitally important
  - Recommendation 51:

    "A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast"

Why is Secrecy Important ?

- Voters do discuss how they voted
- But there is no obligation to do so
- Voters do not have any proof of the way they say they have voted
- Being able to prove the value of a vote

  -> vote buying

  -> voter coercion

  -> election results do not reflect the will of the voters

Norwegian Internet Voting Design

- Lessons from Estonian and Netherlands internet voting systems
- Contains features of secrecy protection and verifiability
- Secrecy protection – repeat voting (as Estonia) but also supremacy of the paper ballot and extended paper voting options
- Verifiability – provision of return codes, plus other mechanisms

The Return Code

- All internet voters sent a return code
  - SMS sent to pre-registered mobile phone
  - Code for party selected and number of personal votes
  - Compare code to list of codes on back of polling card
  - Combination of codes for each ballot entity unique for the voter
- Return code only the first component of overall system verifiability
- Benefits of the return code – verifiability and trust

Return Codes and Secrecy

- Does the return code violate secrecy ?
- Possibility for repeat voting – no guarantee an observed return code represents a counted vote
- Paper voting option – cancel any internet vote by a paper ballot, including option to cast on e-day
- The coercer/vote-buyer will never know if a return code represents a counted ballot
- Secrecy is not violated by the return code

Return Code as a Voting Receipt ?

- CoE rec. 51 prohibits voting receipts
  - "A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast"
- No – can never prove a return code represents a counted vote
- But:
  - Language of the recommendation concerns "vote cast", not counted
  - Rec. 51 relates to the voter, not any third party
  - If not a voting receipt then what value is it to the voter ?
- Initial Assessment – return codes are receipts

A Teleological Approach

- Focus on the intention of the recommendation
- Distinction between the voter and third parties
  - Voter always know if return code is proof of the vote
  - Third party will not know, proof relies on personal knowledge only available to the voter
  - Wording of Rec. 51 does not recognize this distinction
- Intention of the recommendation:
  - Ensure vote buying and coercion not take place
  - Only possible if proof can be given to third parties
- Return code only provides information of value to the voter

Conclusion

- Return codes do represent voting receipts
- Violation of standards under literal interpretation of the CoR recommendations
- Teleological approach allows us to explore the intention of the recommendation
- Intention is to preclude proof of the vote value to third parties
- The return code does not do this, therefore does not violate secrecy standards and Rec. 51

Questions?