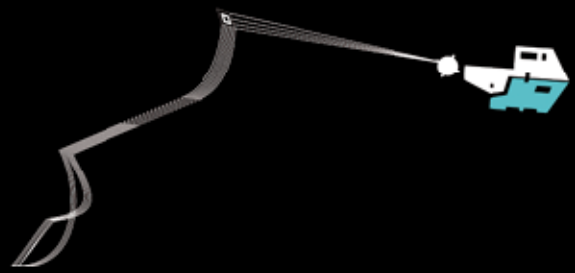
UNIVERSITY OF TWENTE.

Combatting electoral traces

The Dutch tempest discussion and beyond

Wolter Pieters



My background

- Computer scientist & applied philosopher
- PhD Radboud University of Nijmegen
- 2007-2008 Dutch Ministry of the Interior (this work only based on publicly available information)
- Currently postdoc University of Twente

Contents

- The e-voting controversy in the Netherlands
- An actor-network analysis of the tempest issue
- Defining electoral traces
- Combatting electoral traces

The e-voting controversy in the Netherlands

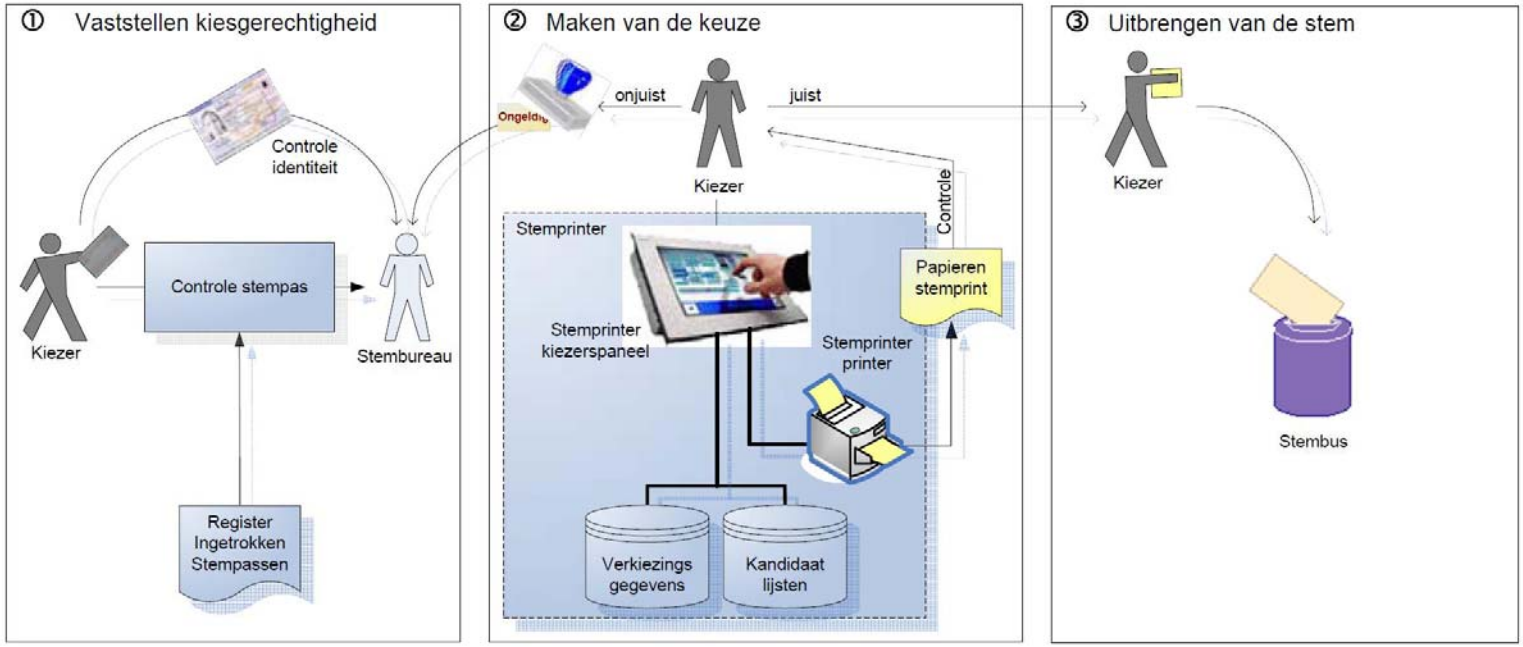
- Why did the Dutch stop e-voting?

Two central themes (wijvertrouwenstemcomputersniet.nl)

- verifiability
  - no paper trail
  - easy replacement of program chips
  - unprotected storage facilities
- secrecy of the vote
  - machines emit radiation (tempest)
  - choice of the voter can be captured with antenna

Proposed solution (Election process advisory commission)

- ballot printer + vote counter, with OCR
- does not solve tempest issue
- e-voting abandoned

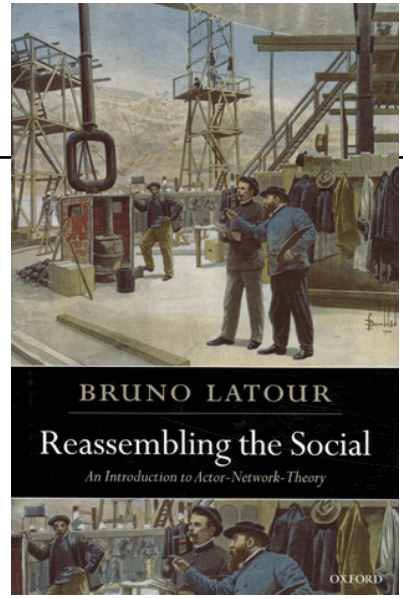


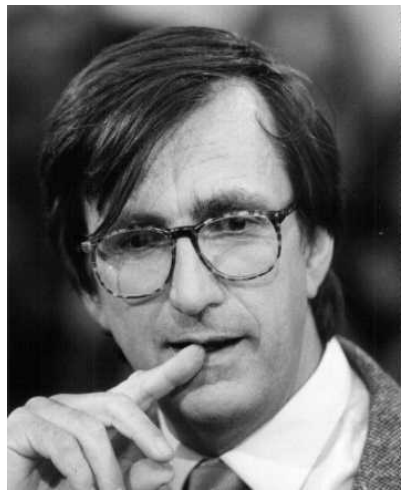
An actor-network analysis of the tempest issue

- How did compromising radiation become so prominent in the Dutch debate?

Actor-network theory

- Bruno Latour
- sociology of associations
- symmetry of humans and nonhumans
- “flat landscape”
- mediation, translation, delegation
- example: hotel key





The alliance of tempest supporters

- Nedap: our machines have a particular feature that switches the display mode in case of special characters
- CDA: we actually have a special character in our name
- pressure group / media: radiation problem easy to show
- government: verifiability is not in the law; secret ballot cornerstone

http://www.youtube.com/watch?v=B05wPomCjEY

- focus on tempest in risk perception
- technical detail translated into public problem

The alliance of tempest supporters

- tempest issue with NEDAPs easy to solve (remove special character)
- intelligence agency: we can *measure* radiation
- Sdu: we have a voting machine with even worse tempest behaviour
- government: such machines are decertified
- problem with particular machine translated to *the* e-voting problem

Inside or outside?

- Minister: capturing *outside* the polling station not a problem, because attacker doesn't know who votes; capturing *inside* without detection is concern
- physically, radiation is believed to decrease quadratically with distance: signal inside will always be stronger than outside
- recasting the inside/outside problem so that *outside* is the most dangerous makes sense from a physical perspective!
- Minister: capturing *inside* the polling station not a problem, because it will draw attention; capturing *outside* is concern

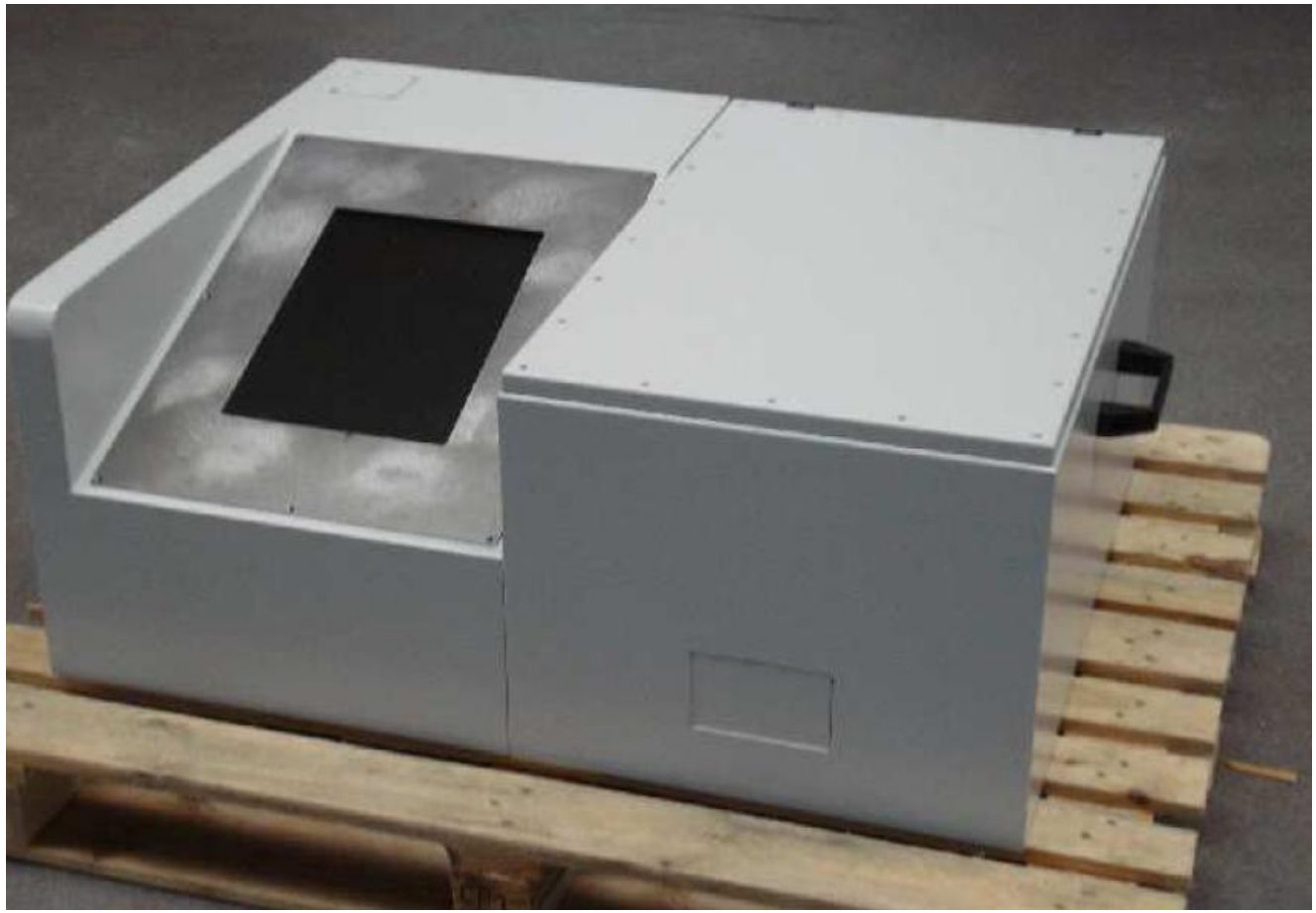
From measurement to norm

- Sdu machines radiate (detectably) up to 40 metres; Nedap machines have *actual* (measured) radiation range of 5 metres
- “As I said before in parliament, there remains as a residual risk the possibility that radiation from the machine can be captured and the display reproduced within a range of maximum 5 metres. This, however, requires very advanced devices. As I stated in the AO [discussion with parliament] of 31 October 2006, I hold the opinion that this residual risk is acceptable.”
- “maximum” can be read descriptively or normatively
- parliament will now only accept this maximum range; mediation of actions by text; actual range has been translated into norm

From organisational to technical

- Electoral Council: reactive measures insufficient
- Electoral Process Advisory Commission: preventive measures advised if costs not prohibitive; secrecy of tempest norms problematic
- assignment to GBS: make a public standard
- expectation of technical solution reinforced by assignment!
- final physical translation of 5 metre norm: radiation can be captured from at most 5 metres distance with antenna aperture of 1 m^2

A tempest-proof vote printer



From technical to organisational

- compliant devices would have heavy shielding (transport!)
- tempest measurement requires:
  - accreditation of each *type* of machine
  - each *individual* machine tested every 2 years for 25 minutes
  - 50 weeks of testing!
- software excluded from testing

- conclusion: a *technical* norm would be impractical from an *organisational* point of view!
- Expert Group advised against ballot printer

Defining electoral traces

- How can we generalise from the Dutch experience to aid future risk analysis?

Internet voting?

- observation: the tempest problem did *not* affect the Internet voting discussion!
- why?

Electoral traces

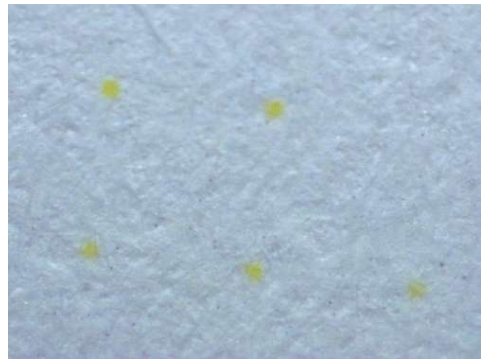
An electoral trace is a piece of information (partly) revealing the connection between voter and vote.

- marking the voter
- marking the vote

- digital
- physical
- social

Examples

- tempest
- fingerprints
- printer memory
- “yellow dots”
- exit polls
- camera recordings
- family voting



Attributes of electoral traces

- added value
- context
- domain
- effort
- information content
- intentionality
- (c)overtness
- persistence

“Ideal” situation

- identify electoral traces of an election system
- classify and compare electoral traces
- decide what is acceptable based on such a comparison

- Internet voting: worse electoral traces than tempest (and harder to capture)!
- implicit in discussion

Combatting electoral traces

- Which measures can be taken to reduce the risks associated with electoral traces?

Technical solutions

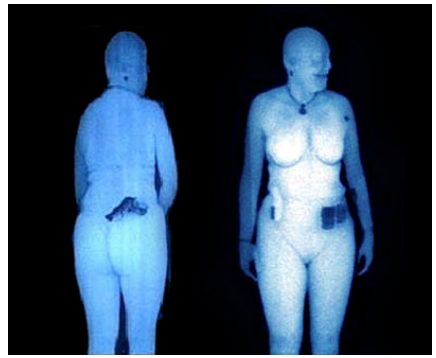
- technical measures
- norms
- certification

e.g. tempest, memory-less printing

Organisational solutions

- organisational norms
- enforcement

e.g. requirements for polling station setup, scanning people for electronic devices, separating ballots for different races



Legal measures

- criminal law
- enforcement

Conclusions

- Dutch tempest discussion shows sensitivity of electoral traces
- Can explode because of associations of seemingly insignificant matters
- Actor-network theory can explain development of controversy in terms of associations and translation
  - social environment changes technical detail into public problem
  - physical properties of radiation mediate problem formulation
  - actual radiation range transformed into norm

Conclusions

- Tempest not considered in Internet voting, which can be thought of as rational concerning its other problems
- Framework needed for comparing electoral traces
- First investigation of relevant concepts & measures

Fokke & Sukke find it very useful

- And the good thing is: you're not only finding out how someone voted…
- … you're also getting traffic info!

Workshop on Security and Privacy in Cloud Computing (SPCC2010, www.spcc2010.info)

Conference on Computer Privacy & Data Protection (CPDP)

Brussels, 29 January 2010

Keynote: Prof.dr. Jean-Pierre Seifert, TU Berlin & Deutsche Telekom

Submission deadline: probably November 16

Organised by Twente, Nijmegen, Eindhoven, Luxembourg

Challenge:

How to apply notions of verifiability from e-voting to cloud computing?

Get your draft CFP here