Internet voting. Then what? Some reflections on trust and expertise.

David Monniaux

CNRS / VERIMAG

2021-11-09

Warnings

Not a social or political scientist.

Work in algorithmics, automated software analysis, automated theorem proving, security, safety-critical systems.

Teaches algorithmics, programming, automated software analysis, automated theorem proving, logic, complexity theory.

A case: Internet voting in political elections

Touted as

- solution to voter apathy
- way to increase the number of elections, referendums per year
- reduce cost of elections and need for volunteers

Now what

Those who lost claim there has been foul play...

(Trump 2020)

What do we do?

Expertise

“Just ask experts to talk about the issues”

We have seen what happens about this with COVID-19!

Who media invites

Generic problems

- **non-experts called as experts**; “essayisme”
- non-scientists presented as scientists
- real experts asked to talk about things outside their expertise

More specific to computing?

The media is likely to call just about anybody (industry PR, “evangelist”, philosopher, sociologist...) except a computer scientist.

Bad perspective

A taste for **clashes**: “for” vs “against”

Very different from scientific disputatio.

Do scientists really know?

A lot on industry topics is **corporate private information**.

Scientists find information in “grey literature”, hearsay etc.

Is this a sound basis for expertise?

Making it personal

(As witnessed in COVID-19)

- "You criticize my fake medicine, you must be a Big Pharma shill!"
- **Threats against researchers**, including junior ones w/o permanent positions.
- Innuendo and conclusions drawn quickly: anybody can be "proved" to have industry connections / conflicts of interests.

Lack of understanding

The public, as well as many journalists and politicians, does not know how science is to be evaluated for soundness.

- lack of understanding (understandable) about mechanisms of scientific publications
- badly understood epistemology (including from bad popular versions of sociology and philosophy of science)
- different standards for explanation, deduction, thought

Different frames of reference.

Back to voting

"Solutionnisme"

Tech bro version

"We can ensure the safety of Internet voting! Just put **everything on the blockchain**!"

More reasonable

"We can ensure the safety of Internet voting! Secure enclave on the voting device, cryptographic protocol for voting with verifiable votes!"

A few sad facts

- Blockchains are touted as silver bullets without concern for relevance.
- Microarchitectural side channels, speculative execution attacks etc. on secure enclaves make fascinating discussion (but not for the general public) and new holes are likely.
- Definitions of safety in cryptographic protocols: for **people with master degrees or doctorates in mathematics / computer science**.

How do we talk to the population about this if we have a conspiracy theorist or a guru against us?

Complexity

Security in computer systems often adds to complexity

- complicated cryptographic protocols
- key management
- microarchitectural isolation

Complexity is bad for

- Reliability
- **Understanding by the general population**

Prefer a simple explanation: “you’re being scammed”

In short

In a climate of fake news, polarization, moral panics ("islamo-leftism"), is it reasonable to add crisis potential to election outcomes?

I don't think we scientists can handle it.