Democracy, Security and Evidence let's have all three

ASIACRYPT 2018

Vanessa Teague

University of Melbourne

December 5, 2018

Secure voting system designs predate computers

Actually, they predate paper too.

- The votes are private.
- The election result is publicly verifiable.

image: Sharon Mollerus. https://commons.wikimedia.org/wiki/File:Athenian_Secret_Ballot.jpg

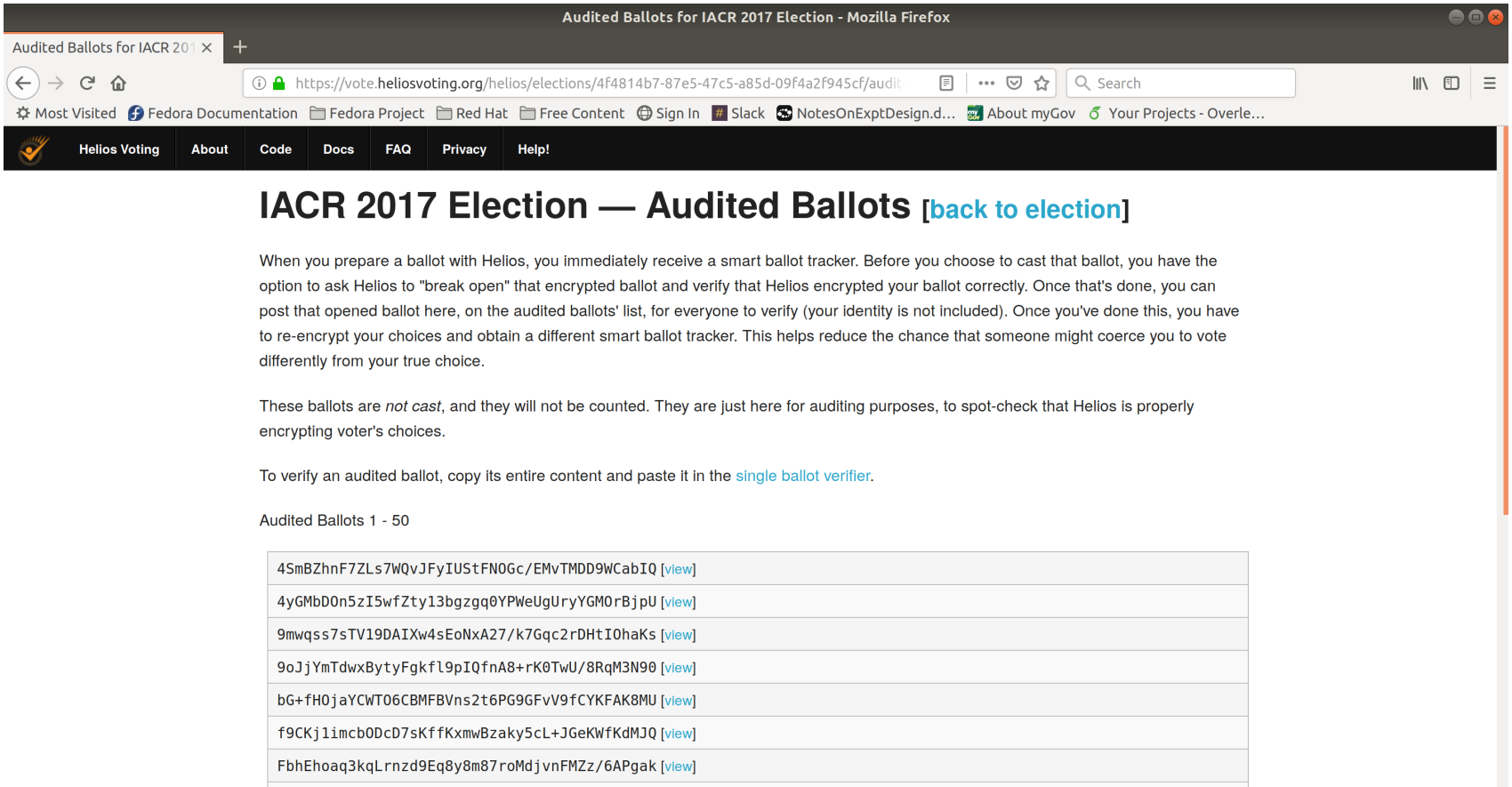
End-to-end verifiability

1. Voters can check that their vote is cast as they intended and
2. included in the count.
3. The election result is publicly verifiable.

Helios

Used in IACR elections.

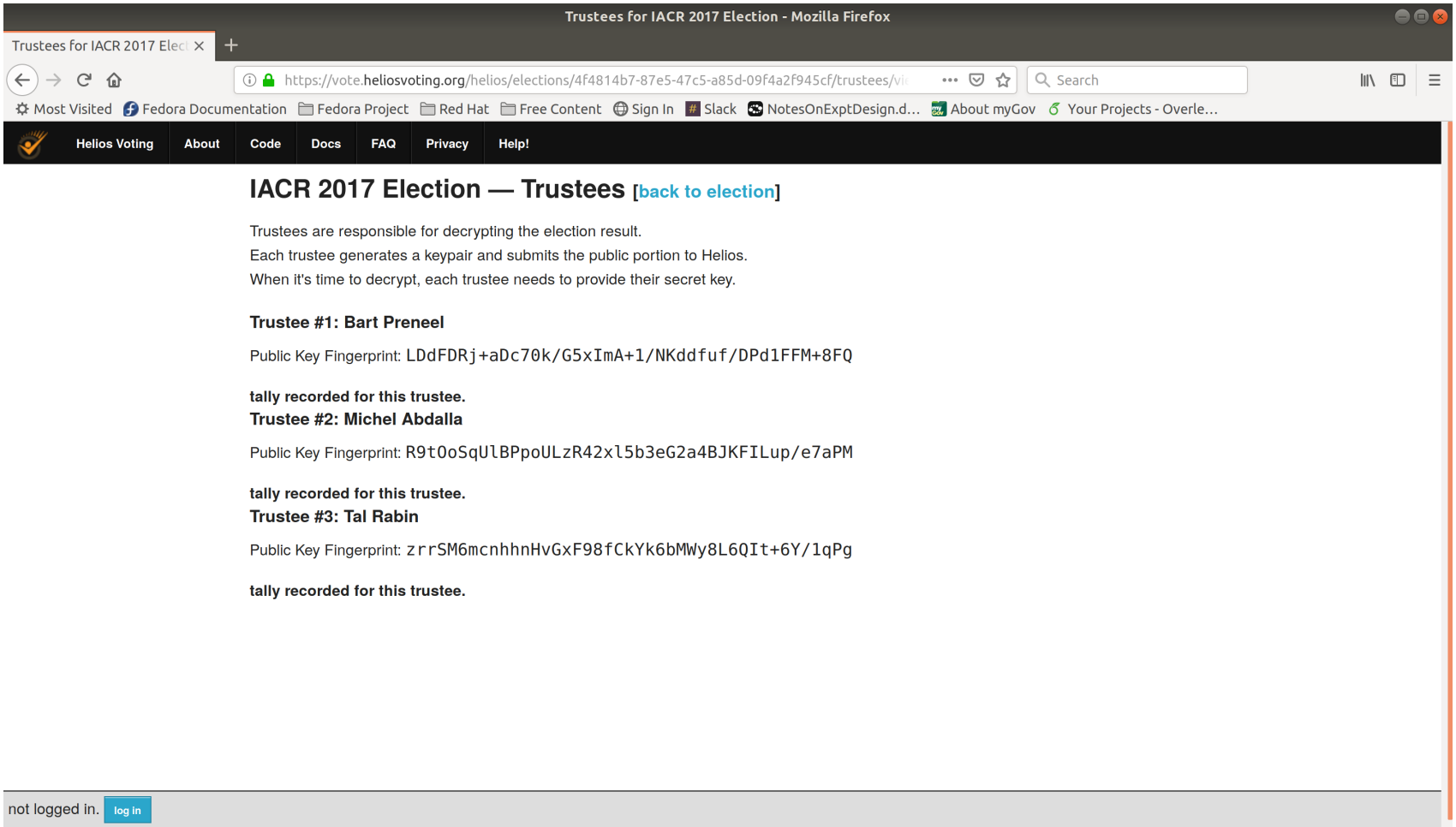
1. Voters can challenge ciphertexts and demand to see the randomness used to generate them, which can then be confirmed using another device. They cast one they haven't challenged.
2. Voters can look up the ciphertext on a public bulletin board.



Helios (cont'd)

Used in IACR elections.

3. Votes are added using homomorphic encryption. The total is decrypted and proven correct with ZKPs.



Known attacks, weaknesses, etc.

1. It's not receipt-free: you can remember the randomness used to encrypt your vote, and thus prove what you cast.
2. Voters could be tricked into not verifying properly.
3. Voters could be tricked into going to the wrong website.
4. Voters could be tricked into not looking at the real bulletin board.
5. Some older variants are vulnerable to the "clash attack," in which ≥ 2 voters think the same vote is theirs. (This is fixed by generating IDs carefully.)
6. ...

What is evidence exactly?

- Is it enough for the result to be verifiable, or should we insist that it be verified?
- What if none of the (other) voters bother verifying?
- Do we need statistical confidence, *e.g.* from Risk-Limiting Audits of paper ballots?
- Or does the possibility of getting caught disincentivize cheating?

What is evidence exactly?

- Is it enough for the result to be verifiable, or should we insist that it be verified?
- What if none of the (other) voters bother verifying?
- Do we need statistical confidence, *e.g.* from Risk-Limiting Audits of paper ballots?
- Or does the possibility of getting caught disincentivize cheating?

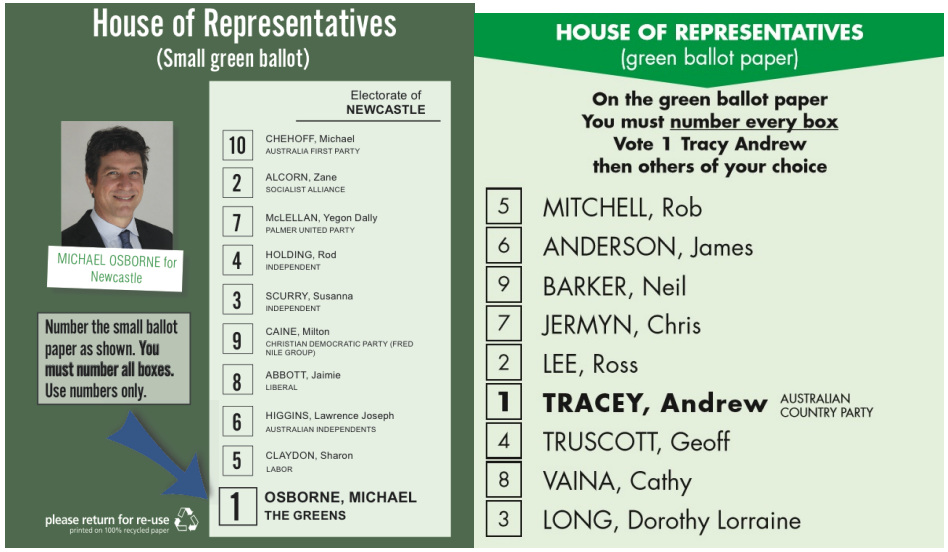
My two cents: it's a little like Popper's definition of a scientific theory. An election process that is verifiable might still give you a wrong answer (if nobody verified), but an election process that's not verifiable isn't an election process at all.

What would you do if you were running this in Australia?

e.g. our paper on privacy-preserving tallying of preferential votes (which can't be counted by addition).
with Kim Ramchen, Chris Culnane and Olivier Pereira:
`https://eprint.iacr.org/2018/246`

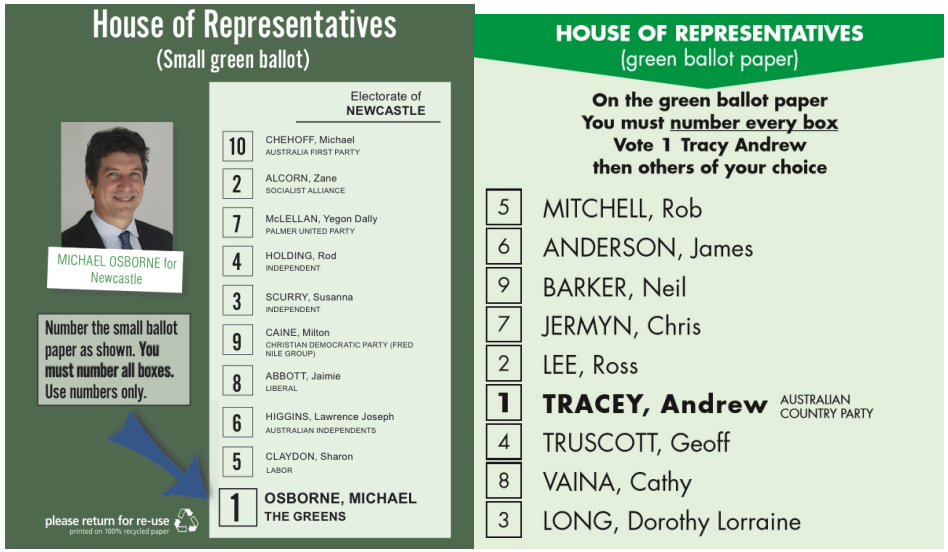
Instant-runoff Voting (IRV)

Used in Australia, Canada, India, Ireland, U.K., U.S., . . .



Instant-runoff Voting (IRV)

Used in Australia, Canada, India, Ireland, U.K., U.S., . . .



Counting process (single winner):

1. Count votes, using 1st preference only
   If a candidate gets majority, he wins
2. Remove candidate with lowest number of votes
   "Shift left" the ballots that contained a vote for that candidate
   Go back to 1.

images: `http://www.firearmscouncil.org.au/wp-content/uploads/2016/06/McEwen-ACP-HTV-1.jpg`
`http://www.newcastlegreens.org.au/wp-content/uploads/2013/09/House-of-Reps.png`

Publishing complete votes causes a privacy problem

- Because the number of permutations can be much larger than the number of voters.
- So the coercer demands a particular permutation and then punishes the voter if it doesn't appear.

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

- Fully homomorphic encryption still looks expensive/cumbersome

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

- Fully homomorphic encryption still looks expensive/cumbersome
- Secret sharing based verifiable MPC solutions [BaumDO'14] use
  - secure channels between voters and trustees
  - distributed key generation (not fully threshold) in covert adversary model

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

- Fully homomorphic encryption still looks expensive/cumbersome
- Secret sharing based verifiable MPC solutions [BaumDO'14] use
  - secure channels between voters and trustees
  - distributed key generation (not fully threshold) in covert adversary model
- Threshold public key encryption based solutions rely on:
  - RSA moduli with unknown factors [CramerDN01, SchoenmakersV15]
    $\Rightarrow$ key generation cumbersome

Somewhat Homomorphic Encryption with Encryption Switching

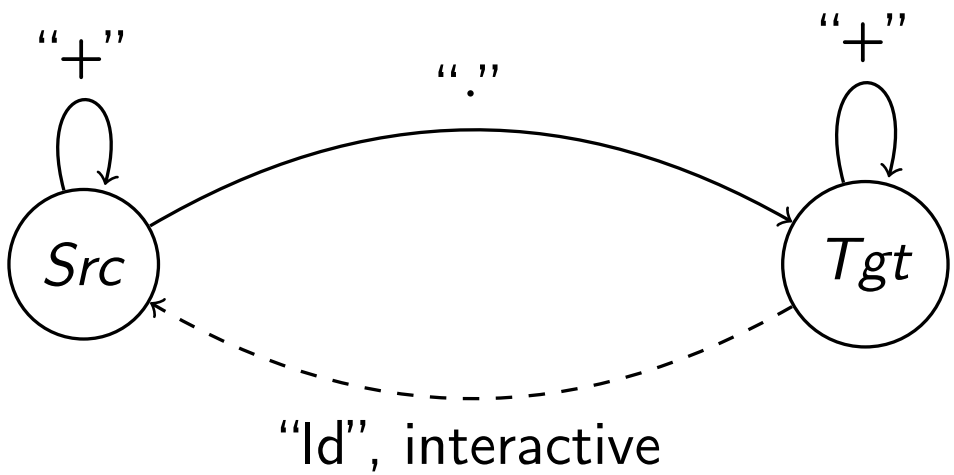
Our solution:

- Design a somewhat homomorphic encryption scheme with threshold key generation in the malicious adversary setting
  $\Rightarrow$ we can do many "$+$" and one "$\cdot$" (then more "$+$")
  [BonehGohNissim05, CatalanoFiore15]

Somewhat Homomorphic Encryption with Encryption Switching

Our solution:

- Design a somewhat homomorphic encryption scheme with threshold key generation in the malicious adversary setting
  $\Rightarrow$ we can do many "+" and one "$\cdot$" (then more "+")
  [BonehGohNissim05, CatalanoFiore15]
- Design a multi-party encryption switching protocol from *target* space to *source* space
  $\Rightarrow$ after switching, we can do one more multiplication!

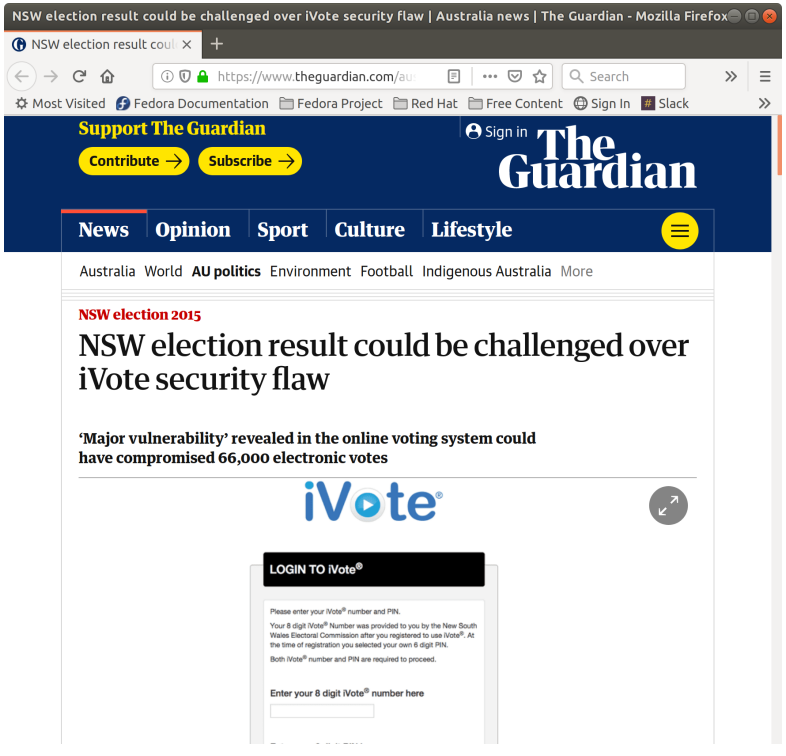


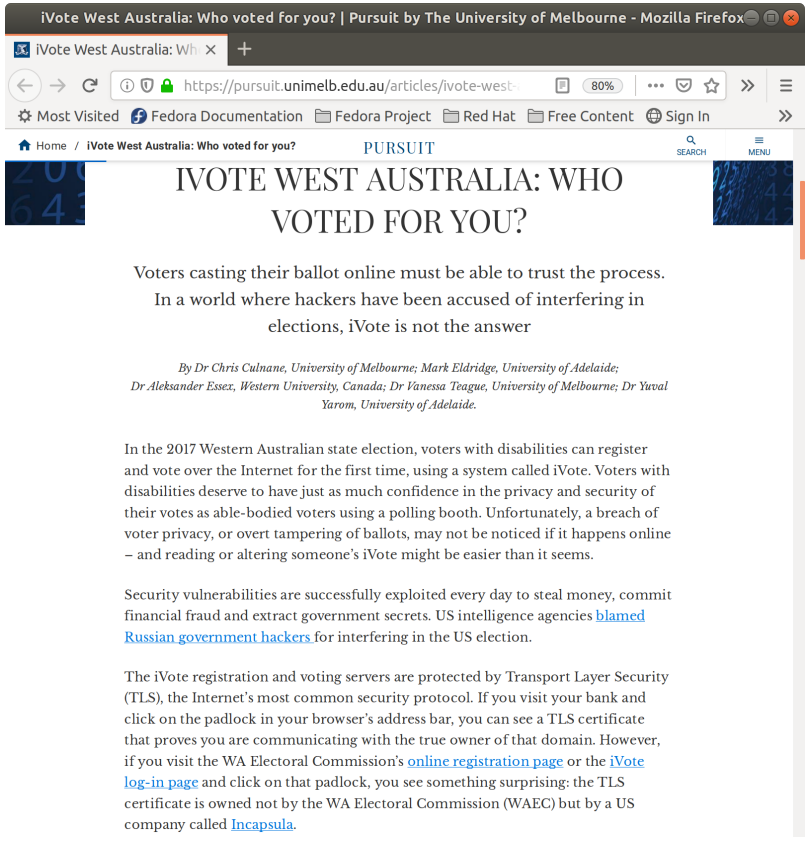
What actually happens when Internet voting runs in Australia?

- The Australian State of New South Wales runs an Internet voting system called iVote.

What actually happens when Internet voting runs in Australia?

- The Australian State of New South Wales runs an Internet voting system called iVote.





Is it end-to-end verifiable?

- "Verification" consists of telephoning an automated system that reads back your vote to you.

Is it end-to-end verifiable?

- "Verification" consists of telephoning an automated system that reads back your vote to you.
- The Electoral Commission said after the election that "Some 1.7% of electors who voted using iVote® also used the verification service and none of them identified any anomalies with their vote."

Is it end-to-end verifiable?

- "Verification" consists of telephoning an automated system that reads back your vote to you.
- The Electoral Commission said after the election that "Some 1.7% of electors who voted using iVote® also used the verification service and none of them identified any anomalies with their vote."
- A year later they admitted that about 10% of calls hadn't been able to retrieve any vote at all.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- iVote is used only for a small fraction of votes (about 6%),

[1] But we should add some verifiability.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- iVote is used only for a small fraction of votes (about 6%),
- therefore nobody will bother to attack it,

[1] But we should add some verifiability.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- iVote is used only for a small fraction of votes (about 6%),
- therefore nobody will bother to attack it,
- therefore it is secure in a realistic attacker model,

[1] But we should add some verifiability.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- iVote is used only for a small fraction of votes (about 6%),
- therefore nobody will bother to attack it,
- therefore it is secure in a realistic attacker model,
- therefore it should be expanded nationwide.[1]

Report at `http://www.elections.nsw.gov.au/about_us/plans_and_reports/independent_reports/report_on_the_ivote_system`

[1] But we should add some verifiability.

What about academic concerns re large-scale undetectable electoral fraud?

"The key difficulty I have with this argument is that it places too much weight on theoretical possibility and not enough on empirical likelihood, or probability of things occurring."

Did I promise not to mention the Telecommunications Assistance and Access bill?

[The Opposition said] the bill was still "far from perfect and there are likely to be significant outstanding issues."

What can we do?