


# Submission on the 2023 Australian Cyber Security Strategy Draft

A/Prof Vanessa Teague  
Thinking Cybersecurity Pty. Ltd.  
and the Australian National University



April 14, 2023

Australian cybersecurity law, policy and practice are such a mess that the security of our nation is at risk.

Australia has some of the most invasive “national security” laws in the democratic world, including compulsory ID checks for SIM card purchases, forced takeovers by government of critical infrastructure, forced “acts or things” that persons with knowledge of computer systems can be compelled to undertake, and Technical Capability Notices, which allow authorities to force corporations to gather extra user data that they would not otherwise collect. None of this seems to have made us more secure. On the contrary, some of these laws have directly contributed to data breaches, such as Optus’s leak of the identity documents it was compelled by law to acquire.

We need to choose different behaviours in order to achieve better results.

Our nation would be more secure if Australia’s cybersecurity policy was refocused around three themes: **democracy, honesty and learning.**

# 1 Democracy

When the Cybersecurity Strategy Draft Policy says that “Our ambition to become the most cyber secure nation by 2030 can be balanced with our liberal democratic values,” it buys into a notion of “balance,” a tradeoff between democracy and security, which is essentially what the Chinese Communist Party invokes when they imprison journalists.

Democracy does not need to be sacrificed in order to buy security. On the contrary, greater government transparency and accountability, along with stronger protections of individual human rights including privacy rights, make us all more secure. The confusion results from the conflation of security with ubiquitous surveillance, which is indeed inconsistent with democratic values.

Invasive surveillance laws are bad for democracy and also bad for security. Australia’s requirement that communications providers store identification documents for phone customers contributed directly to the Optus data breach, which put millions of Australians’ identity security at risk. Perhaps it also helped police to catch some criminals, but it needs to be urgently reassessed given the demonstrated heightened risk to millions of non-criminals—overall, this rule probably makes us less secure.

Similarly undemocratic provisions in the ASIO Act 1979, the Telecommunications Act 1997, and the Telecommunications (Interception and Access) Act 1979, allow for forced alteration of systems to extract information. These may occasionally catch criminals, but may also undermine the security of communication networks. Currently, these provisions are highly invasive, may do collateral security damage to completely innocent people, and do not have adequate restraint or reporting requirements for us to be confident that they do not facilitate more crime than they prevent.

Critical infrastructure protection sounds good, but critical infrastructure forced takeovers could also undermine security if they are misguided or botched.

Rather than “balancing” democracy with security, we can improve both security and democracy by limiting surveillance.

- Repeal or substantially amend legislation focused on surveillance rather than security, including
  - metadata retention, particularly the ID document requirements,

- defence export controls, at least to make an exemption for fundamental scientific research, especially in encryption and security,
  - the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, particularly Technical Capability Notices,
  - the deliberate undermining of strong authentication from the “Identify and Disrupt” amendments to the telecommunications Act, and
  - the various clauses allowing ASIO or others to force an innocent “person with knowledge of a computer system,” to do things they do not wish to do, particularly those clauses that do not require a warrant from a judge.
- Encourage the ubiquitous default use of end-to-end encryption, ad blockers, two- or multi-factor authentication and other privacy- and security-preserving technology. These require both funding to build the products and advertising campaigns to get people to use them.
  - Strengthen legal protections of personal data, and stop sharing or selling “de-identified” data if it can be re-identified. (I have already made a submission to the Privacy Act Review and will not repeat the details here.) Protecting personal data is critically important to protecting both individual security and Australian National Security.

## 2 Honesty

Honesty starts with openness about government processes, including openness about technology, protocols and code. Honesty about problems, weaknesses, shortcomings and mistakes is also critically important.

Transparency about technology allows serious problems and weaknesses to be identified before they cause trouble, or at least reduces the amount of time they remain live. The Australian habit of keeping source code secret and claiming “security implications”<sup>1</sup> is doing nothing for security.

---

<sup>1</sup>See for example the AEC’s response to a question about whether the source code for the Senate count is open: <https://twitter.com/AusElectoralCom/status/1536514421371338752?s=20>

We were able to find serious cryptographic problems in the NSW iVote system because the vendor sold a closely related system to Switzerland, which has transparency rules for voting software [HLPT20]. NSW legislation mandating source code secrecy protected neither the security of the system nor the reputations of its proponents. The Swiss Federal Chancellery responded to our discoveries by doubling down on openness and expert input—they paused Internet voting and funded an extensive program of open, expert examination of the system’s specification and source code.<sup>2</sup> The NSW government did nothing, and the NSW Electoral Commission continued to run the system until it crashed and disenfranchised thousands of voters.<sup>3</sup> Which of these approaches made the democracy more secure?

Denial was also the strategy of Services Australia in response to a demonstration that their voice-based Authentication method is insecure. A Guardian investigation<sup>4</sup> states

Toby Walsh, the chief scientist at the University of New South Wales’ AI Institute, told Guardian Australia he was able to clone his own voice within five minutes, and the ease with which AI could bypass biometric identification showed its limits as a security tool.

Yet Services Australia responded to this demonstration of a vulnerability, by two respected journalists and one of Australia’s leading AI researchers, with a claim that ‘voice ID is a “highly secure authentication method,”’ which is clearly not true.

A more honest approach to systems, source code and security problems would make us all more secure.

- Be honest and open about technology, for example open the source code for the Senate count and the myGovID system, both of which are owned by public authorities.
- Be honest about problems, for example acknowledge that patients are identifiable in the published Medicare-PBS dataset from 2016 [CRT17],

---

<sup>2</sup>Including paying us to continue working on it: [https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung\\_systeme.html](https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html)

<sup>3</sup><https://www.abc.net.au/news/2022-03-17/ivote-revote-ordered-supreme-court-judgement/100917050>

<sup>4</sup><https://www.theguardian.com/technology/2023/mar/16/voice-system-used-to-verify-identity-by-centrelink-can-be-fooled-by-ai>

and that the authentication security problems identified in Services Australia’s voice authentication are serious.

- Be serious about fixing problems. Denying them does not make them go away.

Hiding cybersecurity problems from the public is not just undemocratic. It is also a missed opportunity to earn public trust by telling the truth. Even more importantly, refusing to acknowledge that something is broken makes it impossible to learn how to fix it.

### 3 Learning

Many democratic countries are doing cybersecurity better than Australia. We can learn from Switzerland, Taiwan, Estonia and others. All of them are as small as (or much smaller than) Australia, and all of them have a commitment to democracy and honesty that we could learn from. (None of them are perfect—Estonians place far too much faith in their Internet voting system, for example.)

For example, the Estonian digital identity system is an inherently privacy-preserving design based on a well-designed cryptographic protocol. It isn’t perfect, but its security and privacy guarantees are vastly superior to those of Australia’s Trusted Digital Identity Framework. We could learn how it works and think about building something similar.

- Support advanced technical teaching at universities and TAFEs. We need a large, diverse set of Australians to get real skills on the technical side of cybersecurity.
- Make a genuine commitment to excellence in STEM from primary school upward.
- Roll out ongoing public education, from primary school right through to elderly adults, about how people can protect their security and privacy online.

When the HIV/AIDS epidemic first appeared, the Australian government funded a broad, intelligently designed education campaign about safe sex, which was highly effective in keeping Australians safe. Now

that we have an epidemic of cyberattacks, scams and privacy problems, there is almost nothing. Australians are actively discouraged from using privacy-preserving technologies such as end-to-end encryption because it suits some political agendas to demonise it. Technologies such as encryption, ad blockers and TOR are rarely mentioned by government, and often negatively when they are.

Education about online security and privacy should start in schools—show children how to turn off location services, restrict app permissions on their phones, give false information about themselves when true information is not necessary, and download privacy protecting technology such as the Firefox browser and the Signal end-to-end messaging system.

The Australian government could use Facebook and Google microtargeting to send messages about security and privacy to the Australians who are most vulnerable. (You can bet that malicious actors have already found Australia’s most vulnerable people on Facebook.)

- Australia could learn from other democracies that are doing better.

The Australian government could learn from Australians who know about cybersecurity. Home Affairs needs at least one person with expert cybersecurity knowledge on your cybersecurity expert advisory board. Many of us would be happy to help. Everyone wants to see Australia’s cybersecurity improve, which will require a complete reorientation of Australian cyber policy. Democracy, honesty and learning are positives for improving our security.

## References

- [CRT17] Chris Culnane, Benjamin IP Rubinstein, and Vanessa Teague. Health data in an open world. *arXiv preprint arXiv:1712.05627*, 2017. <https://arxiv.org/pdf/1712.05627.pdf>.
- [HLPT20] Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 644–660. IEEE, 2020. [https://dial.uclouvain.be/pr/boreal/object/boreal%3A223906/datastream/PDF\\_01/view](https://dial.uclouvain.be/pr/boreal/object/boreal%3A223906/datastream/PDF_01/view).