

**From:** [REDACTED]  
**To:** [Assistance Bill Consultation](#)  
**Subject:** Assistance and Access Bill  
**Date:** Monday, 10 September 2018 9:07:18 AM

---

G'day,

I'm pleased to have an opportunity to comment on this, but I'm bemused by the process.

<https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018>

says:

The Government welcomes your feedback. Submit any comments to [REDACTED] by 10 September 2018.

but I would have expected a parliamentary committee, not a government department, to be conducting the consultation.

Am I wrong? is this normal? or does this process illustrate yet another new power of Interior and Heimat?

Will the public be able to see the deliberations of this consultation? How are our contributions scrutinised and evaluated? Will there be hearings? a public report?

here I offer my comments as a user (citizen) and a implementer (professional) of applied cryptography.

I welcome acknowledgement that the laws of mathematics are not only commendable, but universal, and so *"communications providers cannot be compelled to build systemic weaknesses or vulnerabilities into their products that undermine the security of communications"* any more than airlines can be compelled to defy gravity, or property developers to defy rising sea levels.

and that's a good thing. Reliable secure cryptography is of great value to all who use it, knowingly or not, on a constant basis.

That's why it is unwelcome to consider requiring technologists to weaken the systems around reliable cryptography, or to further empower law enforcement to covertly access our systems.

While I acknowledge the 'challenges posed by encryption', I also recognise the CSA trope as the same which was employed to justify assaults on the rights of Territorians under the NTER, and the abolition of an entire tier of government in the NT under SuperShires - all without one CSA arrest. Yes, the scenario posed is likely. No, sabotage of public infrastructure is not the best way to address it. Our experience with NTER has demonstrated how those who use CSA to justify other agendas do so at the expense of the victims they claim to be interested in.

Even if the Big Brother being constructed in this new renegade department were benevolent, the deliberate construction of structural weaknesses and points of access in systems surrounding reliable cryptography offers new vectors for other malicious actors.

As a technologist, I am shocked at the thought of being compelled to contribute to this

wrong direction. What other professions are subject to such extreme requirements under such oppressive penalties?

I recommend denying this bill. And furthermore, dismantling the Home Affairs empire before that becomes any more difficult.

I am sorry I couldn't make time to give this bad new bill the detailed response it deserves within the suggested timeframe.

Justin Tutty

[REDACTED]

. . . *justin* <\*> [REDACTED] <|> [REDACTED] J: {} }