

From: Peter Dolkens
To: [Assistance Bill Consultation](#)
Subject: URGENT: Important message to the people who don't understand basic mathematics but are currently in charge of the circus we call "The Australian Government"
Date: Monday, 3 September 2018 10:00:36 AM

Hi,

I am grossly concerned by the latest assistance and access bill.

It demands things which compromise the fundamental security of individuals both in Australia, and abroad.

If I were to tell you that you need to leave a copy of your bank card, and PIN at my place, just for safe keeping, how would you feel about that? The Australian government has demonstrated numerous times (can anyone say census without getting fired yet?) that it is technically incompetent, and I don't wish to place my livelihood, identity, and security at that kind of risk.

The only certainty there is in computing, security, and mathematics, is that if there is no flaw, it can't be exploited. By demanding companies work deliberate flaws (you call them "master keys" or "backdoors" or "passwords") into our security, you're effectively ensuring that eventually, we will see massive data breaches like the Equifax theft that is **still** affecting millions of people across the world today.

Furthermore, even if I **did** trust you with my information like that, the legal requirements surrounding the use of that data simply do not stand up to any reasonable standards. Now, I understand that you're very good at using scary sob stories (won't **somebody** think of the children!) to make excuses for why you can't do your job properly, but that's simply not enough. This law does literally NOTHING in ANY of those situations.

Encryption is math, and unless you're going to start locking people up for doing maths (great education program there minister), you simply cannot block encryption. All you can do is weaken the encryption that protects the average citizen from criminals. Criminals will still continue to use encryption. Just as they have done since the dark ages. Just because you can unlock a device, or access someones private messages, doesn't mean they can't use personal, private cryptography that will block your access anyways. There are even ways to encrypt things in a fashion that provides plausible deniability, such as embedding second and third images within harmless images, for example.

So at the end of the day, your bill does NOTHING for the cases you describe, and yet your bill does **considerable harm** to me as a consumer. You open me and my family up to risks like "the fappening", "cryptolocker", and regular cybercrimes.

All I can say, is that I hope that if this bill goes through, that criminals target you, and every member of parliament that vote for this bill, and use the very same weaknesses and flaws that you are exposing me to, in order to clean out your bank accounts, expose your family secrets, and steal your identities.

Those are the risks you are placing on me, and thus, I wish them back on you tenfold.

Thankyou

Peter Dolkens