| | |
|---|---|
| **From:** | jharrop@gmail.com |
| **To:** | Committee, PJCIS (REPS) |
| **Subject:** | Submission to review of Assistance and Access Bill |
| **Date:** | Monday, 8 October 2018 8:00:18 AM |
| **Attachments:** | submission_PJCIS_Assistance_and_Access |

Submission to review of Assistance and Access Bill follows in text and PDF formats.

Jason Harrop

------------

This is a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 [0].

Chinese surveillance society [1] offers a chilling vision of a society I never want to live in.

Just as Apple differentiates itself [2] clearly from Google and Facebook by saying we will never sell your data (you aren't the product), I think Western democracies ought to clearly differentiate themselves from China.

Currently we're heading towards a local optima that will look more and more like China. Because of certain problems (paedophiles, drug dealers, terrorists), government wants weak encryption. Then in large part because of weak encryption, we can't use Chinese components in our networks [3].

Well, the truth is that paedophiles/drug dealers/terrorists will all wake up to the fact that comms on common services can be intercepted, and will use their own encryption (routed over TOR or similar, so you can't tell who the endpoints are). Phantom Secure is evidence that this horse has already bolted[4]. Though I guess you might make any private encryption technology illegal? Why not?!!

The net result being that only people with "nothing to hide" will be using services that you can surveil.

Thinking more broadly, if drugs such as marijuana and MDMA were legal, then probably 95% of the so-called encryption problem goes away. And lots of other problems as well... Count on certain relatively benign recreational drugs being legalized soon after self-driving cars become common.

And then I'd argue that you catch the paedophiles and terrorists with creative policing[5]. You don't absolutely need this kind of legislation to then get into their phones [6].

In summary, a much better approach would be to support strong encryption (the global optimum), and say clearly we don't want to follow China. With strong encyption right across our telecomms networks, we'd be able to source equipment from Huwaie and ZTE ... Of course, there's the additional concern that the Chinese could stop packet transmission entirely (ie a kill switch), or make it unreliable, but that's a different problem to "they might read our stuff".

The real concern would then be any laptop server[7] or phone made in China (ie most of them) - the terminal devices where stuff must be decrypted for the user to see.

Of course, the problem is that embracing "strong encryption" is anathema to the received wisdom from the rest of the Five Eyes [8], and you need to take a broader perspective to realise it is the right choice for an open society.

[0]
https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018

[1] http://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278

[2] https://www.washingtonpost.com/technology/2018/10/03/apple-ceo-tim-cook-says-giving-up-your-data-better-services-is-bunch-bunk/

[3] https://www.itnews.com.au/news/huawei-zte-banned-from-australian-5g-networks-500708

https://www.itnews.com.au/news/huawei-zte-banned-from-australian-5g-networks-500708

[4] http://www.abc.net.au/news/2018-03-16/afp-seize-phones-as-part-of-phantom-secure-crackdown/9555652

https://www.theregister.co.uk/2018/10/03/phone_ceo_pleads_guilty/

[5] https://en.wikipedia.org/wiki/Task_Force_Argos

[6] "International cybercriminals and Thailand’s porous border",
http://www.nationmultimedia.com/detail/opinion/30354431

[7] http://www.abc.net.au/news/science/2018-10-05/supermicro-malicious-chips-china-australian-government/10342006

[8] https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption