Dear Sir/Madam,

In accordance with the consultation invitation, I offer the following comments on the proposed Assistance and Access Bill 2018.

There is a serious mismatch between the bill's economic benefits and costs. The proposal requires companies to add mechanisms that deliberately weaken or bypass application security. As any such mechanisms are guaranteed to leak into widespread illegitimate usage, there is certain to be substantial cost due to routine leaking of personal information (such as banking passwords or personal details) leading to identify fraud, in addition to the costs of building the mechanisms. The proposal mentions only a small number of investigations where the proposed surveillance is beneficial, and none which could not have been addressed by good old fashioned policing.

It is unacceptable that the legislation has been proposed while ignoring the certainty that the activities it demands of IT companies will be subsequently used for nefarious purposes. Any back-door, gateway, or bypass will potentially be accessible for other extra-legal purposes - the screen&keyboard monitor that catches Dr Evil's messages can just a easily be used by small time fraudsters and crooks against thousands of everyday people.

The proposal very substantially lessens oversight of eavesdropping without any justification. There is no requirement for routine judicial oversight, and access to the scheme can be approved by political appointments (AAT members). No justification has been given why intercepting personal telephone calls requires judicial approval, but intercepting VOIP calls or emails does not.

Disturbingly, the proposal panders to current increasingly authoritarian trends, but offers no balancing democratic forces or public visibility. Although the world moves further from cold-war paranoia, and by all statistics is consistently become safer and safer, the proposed bill protects us from a 1950's James Bond past.

I am perturbed at the unusually short consideration period, and that the proposal is substantially less promoted and less accessible that similar proposals in other fields; for example the proposal is difficult to find and the explanatory documents not available from the proposal page. Together with the short consideration period, it very much looks like there is lots being hidden - the only sensible assumption being that what is hidden would be unacceptable to most people.

There is an unconsidered mismatch between the moral costs of the proposal (such as loss of privacy, lack of trust) and the moral benefits (revenue recovery, obtaining evidence). Given that traditional policing solves most of the issues raised, and that big-data has a terrible record in both law enforcement and privacy, the moral balance is clearly swayed away from the proposed bill.

The proposed bill has stupendously enormous scope. Almost everyone of technical skills or business involvement could be covered by the proposed bill; requests could originate in unrelated jurisdictions; and parties could be required to perform almost any activity ("a thing") including implementing back-doors - despite various MP's claims to the contrary.

Given these points, the only acceptable outcome will be that the proposed legislation is completed dropped, and a fresh, open, public consultation process begun. Australia has had a number of open, public and effective consultations, such as the processes that considered human cloning legislation - this field demands similar consultation.

Yours sincerely,

  Andrew.

Dr Andrew Fry