From: William Uther
To: Assistance Bill Consultation
Cc: [redacted]
Subject: Feedback on the proposed Home Affairs Assistance and Access Bill, 2018
Date: Saturday, 8 September 2018 9:47:56 PM

Dear Sir/Madam,

I would like to submit some feedback on the proposed Home Affairs Assistance and Access Bill, 2018. The summary of my feedback is that I'm concerned about aspects of the bill and would like to see some clarification of some areas, and some extra safeguards in others, particularly around the secrecy provisions.

I am a software engineer. I was a Senior Researcher at National ICT Australia and Conjoint Senior Lecturer at the University of NSW before leaving for industry. I have now been in industry for over five years. For part of that time I have been involved in fraud and abuse detection and prevention for my employer. I am writing this in my personal capacity as a citizen of Australia and a voter in the North Sydney electorate, not as a representative of my employers, current or previous.

The "going dark" concerns that this bill is aimed to address are legitimate, as are the concerns of those pushing back against further police powers. As in many situations, it is important to find a good balance.

My first comment is that there is much discussion in the explanatory memorandum about what will NOT be done under this proposed legislation. It would be good to see more discussion about what would commonly be done. What do the agencies asking for this power expect to be common requests?

For example, in the explanatory text discussion of "Division 7 - Limitations", I note this text: "Likewise, a notice may require a provider to facilitate access to information prior to or after an encryption method is employed, as this does not weaken the encryption itself." When I try to imagine what a common request would be, I imagine Google being served with notices to install modified keyboard applications on specific phones so that every keystroke is forwarded to a listening post. This would allow government agencies to monitor a phone regardless of which encrypted chat apps were being used. Would Google then be in the loop for every request to install the modified keyboard on a phone? Or, once the modified keyboard app is signed by Google, would the agency acquire a copy of the signed, modified app (perhaps from the phone of the first person Google was required to install it on?) so that they can deploy it on other devices without further notice to Google, or warrants/legal oversight. If the latter is possible, then would the original signing of the app by Google be considered a Systemic Weakness or Vulnerability under the act? It certainly appears to be a systemic weakness to me as it gives a party other than the software developer control over a specific bypass to abuse protections for any user(s), not just those named in the original warrants.

There is much discussion of encryption in the explanatory memorandum. It would be good to directly address both a) digital signing (i.e. the technical process that lets your phone know the Google keyboard app was approved by Google and so can work as a keyboard), and b) the control of artifacts that were required to be signed (e.g. the modified keyboard app Google was required to sign in the example above) in the bill and explanatory memorandum. 317E(1)(C) seems to me to cover digital signing, and yet I could not find such signing and its effects discussed in the explanatory memorandum.

As an individual working in industry, I also have some concerns about how this bill might affect me directly: It appears that an individual can be served with a notice separate from the company they work from. As a software developer I might fall under 317C item 6 regardless of whether my employer falls under another item. If such an employee is served with a secret notice that requires them to act against the stated wishes of their employer (and a secrecy provision that stops them from telling their employer), they do not seem to have many meaningful protections. If this is discovered by the company, it is unclear if they could be fired (they're immune from civil liability, but they're being fired, not sued.) And if not fired, their career could certainly be derailed. In essence, immunity from civil liability does not mean immunity from consequences, and that worries me. It would be good to add a requirement that the notice go to the most senior person in the company possible.

I also have concerns about the secrecy requirements in the bill. While much ink has been spilled debating how the proposed powers may or may not be used, it would be most useful if we could see how they end up being used. There is clearly a tension here with the requirement for ongoing operations to be kept confidential. But it is important that a balance be struck. I think the most important change to the bill would be the addition of a statutory time limit on the secrecy requirements around notices. For example, all requests for secrecy must not be longer than, say, 2 years, perhaps renewable once for a further 2 years by court order. After that time there would no longer be any requirement for secrecy about the existence and nature of the notice. There could, of course, be continued secrecy requirements about specific information disclosed under the notice, e.g. proprietary information by a communications provider, or the contents of an end-users communications that were intercepted.

Again on secrecy requirements, if a Technical Capability Notice is received by a company for a new capability, and it has a secrecy provision attached, does that stop the company from announcing that the capability exists once it is built? I think it reasonable that the fact that the request was made may be kept secret, but I believe that companies should always be able to accurately describe their products to their customers. I'm referring here to capabilities in general, not their application in specific cases.

Moving on from secrecy, the terms "systematic weakness" and "systemic vulnerability" are not defined in the bill, and there is limited discussion in the explanatory memorandum. It appears to mean a weakness that applies to all users, but the limits of this are not at all clear. The most I can find is this text, "The reference to systemic methods of authentication or encryption does not apply to actions that weaken methods of encryption or authentication on a particular device/s. As above, the term systemic refers to actions that impact a broader range of devices and service utilised by third-parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data."

In many cases, the weaknesses of a system are not technical weaknesses, but organisational weaknesses. Designing a system to minimize the organisational weaknesses involved in using the system is an important part in reducing systemic vulnerabilities. For example, imagine someone is selling a line of padlocks with serial numbers, and keeping individual master keys associated with those serial numbers. I think this system would commonly be considered a 'back-door' for the padlocks. There is a large amount of organisational overhead involved in keeping track of all those keys. Any individual key would not be a systemic weakness, it would be an individual weakness, but the mere existence of the system as a whole would be a systemic weakness, compared to a system that did not have such keys. This seems to be acknowledged by later text which says, "The mere fact that a capability to selectively assist agencies with access to a target device exists

will not necessarily mean that a systemic weakness has been built. The nature and scope of any weaknesses and vulnerabilities will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required."

The fact that some design weaknesses that affect a whole system are not necessarily considered 'systemic' makes the following statement in the explanatory memorandum surprising, "This limitation ensures that providers cannot be asked to implement or build so-called ‘backdoors’ into their products or services." I'm not convinced. I actually think this is a better trade-off than many I've seen, but this statement appears misleadingly strong and probably shouldn't appear in an explanatory memorandum. As I noted above, a system of master keys is a back door.

Thank you for considering my input.

Sincerely,

Dr William Uther
Software Engineer

[redacted]