| | |
|---|---|
| **From:** | Clarke, Brendan |
| **To:** | Assistance Bill Consultation |
| **Cc:** | [redacted] |
| **Subject:** | The Assistance and Access Bill 2018 |
| **Date:** | Monday, 10 September 2018 5:22:20 PM |
| **Attachments:** | image001.png<br>image002.png |

Dear Minister,

I am writing to express my concerns over the draft legislation titled 'The Assistance and Access Bill 2018', and outline these concerns below.

1) Technical Assistance Requests should also be included in the annual report.
   The currently draft proposal has not requirements for these requests to be reported on.
   For transparency all requests should be reported in the annual report.
2) The scope of the legislation should be further restricted to only the most serious of crimes or threats to national security. There are not enough protections in this bill to stop harassment or spying on group the government doesn't like such as protesters, media scrutiny or opposition parties. The scope of the legislation must be narrowed down to serious crimes only.
3) The definition and description of Systemic Weakness needs to be more precise.
   Section 317ZG Designated communications provider must not be required to implement or build a systemic weakness or systemic vulnerability etc. This definition is overly broad and open to interpretation and hence is open to abuse.

4) The legislation is extremely broad in who it applies to. It includes the entities like carriers or carriage service providers However, it also covers a person that *"… provides an electronic service that has one or more end users in Australia"* This would apply to every website that is accessible from Australia. Furthermore, the legislation also covers an individual if *"… the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end users in Australia"*, which appears to cover every piece of software, game or mobile app, that connects to internet or produces content that is going to be used on the internet. That is an incredibly broad category and it goes further to cover

any corporation that creates software that may run on a device that will be connected to a telecommunication network, irrespective of whether the software itself is intended for use over that communication network.

5) There is not enough oversite of the use of these new powers so they will not be misused.
   This bill would authorise vast new authorities with almost no understanding of the limitations, implications, or oversight mechanisms. It is unclear who could be implicated, what could be requested, what the effects would be, and how oversight would work.

6) Inherent review by the courts Affected people and companies have an avenue to challenge a decision to issue a notice. Judicial review by the courts is available under the Commonwealth Constitution and the Judiciary Act 1903.
   This would be hard to do for individuals or small businesses who do not have the funds to challenge a notice in court. There does not seem to be any details in the act on how this challenge should be handled.

7) This Bill could harm the cybersecurity of systems for all Australians. The current Bill would require companies to provide information about how their systems operate.
   It would allow more people physical access to networks. It would require organisations to test and install new functionality built by the government. These measures would undoubtedly introduce new threats and vulnerabilities into the systems that we all use each day.
8) This Bill would lead to an increase in government hacking: This Bill grants government officials the power to both compel organisations to reveal information about their systems and to make changes to those systems. Combined with the government's new ability to issue warrants to seize information directly from devices, this would empower Australian government agencies to develop and grow their hacking capacities without vital and necessary protections. Any government hacking must come with strong safeguards given the high risk of harm. While the orders issued under this authority must be reasonable and proportionate, there is nearly no limitation to ensure that the government would not use any vulnerabilities it uncovered around the world or share that information with its allies.
9) This Bill would allow the creations of backdoors into end-to-end encryption despite assurances to the contrary: Whilst the Bill does specifically prohibit the government from mandating a systemic weakness in an encrypted system, the ambiguity in the use of the term "systemic" will highly likely be exploited, and will result in less trust in technologies deployed in Australia. It may be that a company could be compelled to use its software update mechanism to interfere with the system of a specific user. Such a function would undermine faith in software updates, leading users not to update. That means more unpatched systems and overall harm to cybersecurity.
10) This Bill is a huge overreach into the fundamental workings of our digital world: As currently drafted, this Bill would authorise vast new

powers to authorities with almost no understanding of the limitations, the implications, or oversight mechanisms. Encryption protocols are the backbone of the digital economy, facilitating every single transaction online. Any attempt to weaken these will be a risk that no other democracy is taking. Strong encryption is essential to the modern Australian economy, and it would be a mistake to deliberately weaken it.

11) Assistance orders (Strengthening law enforcement search warrants)
This section aims to increase the penalties from 2 to 5 years. And for more serious crimes to 10 years) This is a ridiculous and excessive change to the current law.
Increasing imprisonment times is not a substitute for other evidence.
The existing two years for non-compliance is acceptable.

I urge the government to modify this Bill to increase safeguards against misuse and to remove the overly broad definitions. In its current draft form, this bill is open to misuse and will damage the security of systems use in Australia. Due to the nature of the wording and the overreaching powers this will also lead to a lack of innovation and development of new secure systems in the fear that any new business or individual developing new secure communications services may be in breach of the new laws and will add to their cost to comply.
I, and many other Australians, who use digital communications on a daily basis am concerned about the impact on my rights - particularly the right to privacy.

Thank you
Brendan Clarke

[redacted]

**Brendan Clarke**
Systems Engineer – Proxy Operations
IT Service Management and Operations,
IT Delivery Services, Enterprise Services
[redacted]

**Mobile:** [redacted]
**Fax:** [redacted]
**Email:** [redacted]

**MyService SPG:** [redacted]

"If Sleep is a drug; then I have withdrawal symptoms"
----BEGIN GEEK CODE BLOCK-----
Version:3 12
[redacted]
-----END GEEK CODE BLOCK-----