Hello,

It is good to see that the current surveillance framework in Australia is being reviewed. I think everyone can agree that the current laws allow extreme monitoring of Australians, so it's good to see the government reviewing them.

This submission will quickly try and answer the questions raised in the discussion paper in the below paragraphs.

Australia currently does not have enough protections in place for access to information and data. The Identify and Disrupt 2020 bill for example provides law enforcement with excessive overreach. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) has recommend significant changes, which should at least be addressed urgently.

Ideally that law should be removed and Australians should be protected from government surveillance. When we live in a world with constant cyber threats and attacks from foreign states increasing the attack surface with government laws is a bad idea. We should be improving our defences instead of having the government attack it's own citizens. Watching Russian attempt to start a war with Ukraine using cyber weapons and infrastructure attacks only reinforces this. We should not be mandating back doors and weaknesses just so the government can monitor it's citizens.

We should also expand what is considered communication. Any traffic should be considered communication, no matter the content. That is all communication should be considered content. Metadata for example is extremely informative and sometimes can provide more information then the original message. This would also protect our future technology advances, such as artificial intelligence or quantum computing.

Similarly it shouldn't matter if the data is live or stored, it is critical to protect all information from adversaries and the government. All information should be off limits without very strict judicial oversight and only in narrow cases. For example only for the individuals in a relevant investigation, not all users of a platform.

There should be no special requirements for Australian providers, this just disadvantages Australian companies. Instead all retention requirements should be removed. Retention requirements just collect valuable data in a single place, allowing other nation states easy access. As mentioned above be should be making ourselves more resilient to external threats, not less. The same with warrants, again they should not require back doors or forced vulnerabilities as this puts Australians and Australian companies at risk.

The use of surveillance devices should require a warrant. In a free society a warrant less surveillance program can not be justified. Adding to that a persons location and movements are very private matters. A persons movements can reveal a lot about them, if they are having an affair, their current medical status, their religion or political beliefs and lots of other private information. Previous location data can also be used to predict someone's future movements. That is very scary for domestic violence victims, celebrities, or children all of whom rely of attackers not knowing where they will be. There should be a very high threshold in order to obtain location information.

Warrants should be targeted at persons not only in the first instance, but in all instances. Warrants should also be issued by judges and ASIO warrants should be reviewed by judges. On top of that all data collected should be deleted after a specified time period. The entire process should also be open and transparent, so that the public knows how many and what types of warrants are being issued. The public should also be able to see all warrants after the investigation completes, this way the government can be checked and balanced.

Oversight is extremely important for public trust. Judges and parliament should be conduction regular reviews and the information should be made public as soon as it can be.

The current framework is hurting Australian tech competitiveness. There are no large technology companies that start and remain in Australia, partly due to our tough stance on companies. A large number of multinational companies won't hire Australians as they are worried about excessive government overreach. We need to address this to improve our international competitiveness. On top of that international companies can't comply with the impractical warrants anyway, so we just hurt Australians and don't provide protections.

Finally, all data generated by "Internet of Things" should be protected, as all data should be. As mentioned earlier all accesses of Australian's data should be revealed to the public.

In general I think more emphasis should be spent on increasing the resilience of Australia's technology sector instead of focusing on monitoring. In a potential future conflict, having large databases of Australian movements, faces, personalities or any other information will be used against us. As well as that mandated back doors or vulnerabilities will also be used against our citizens and critical infrastructure. We know from history that databases cannot be kept secure, even by intelligence agencies, so we should limit it's collection in the first place.

Overall it's good to see there is a review. The paper asks some useful questions, all Australians are hoping that the answers end up matching the freedoms and rights that Australians expect. Let's hope that Australians end up being treated more like citizens instead of suspects.