Submission No 84

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Alan William O'Neill

Submission

A number of the proposals in the paper '**EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS'** are practical workarounds to issues that actual flow from a fundamental problem with the Industry and network structures, that are in fact common around the globe. This submission aims to ensure that the debate fully includes an understanding of these fundamentals.

Today's Internet in Australia is comprised of a large number of network providers supplying routed (ie..Internet protocol level) services to enterprises, other networks, application/content providers and consumers. Each network peers for routing and packet forwarding purposes to selected partners over international links, domestic links and at neutral interconnect points. Internet packet routing and forwarding are commodity activities with low barriers to entry, large skill resource, and a commodity equipment/supplier environment. The value in the Internet is primarily added by software, servers, applications and content that are interconnected over this commodity layer. At the same time, and as fully recognised in the above paper, the Internet is now a mission-critical infrastructure for the country with its performance, security and stability as important to national well-being as the road network and basic utility supplies.

The commercial structure of the Australian Internet places our Internet borders, and the defence of attacks against the national Internet, in the hands of commercial organisations with little or no commercial benefit (in fact a significant cost and liability) for the national defence of that network. Further, through a number of court proceedings it has been the position of the industry that what is included in Internet Packets is beyond the responsibility of the provider and they cannot be held responsible for it. This can be viewed as a ' if we don't look and don't see then it cannot be our fault'. This problem with the mindset of one provider is dramatically amplified when it is considered that a network of such providers forms the national internet, and they therefore have a lack of procedures and capabilities for dealing with criminal, security and internet attacks across their networks. Of course, they do indeed have some procedures between them, and through the support of volunteers and government agencies, they can act somewhat together in defence of internet viruses, Denial of Service, and other forms of technical attacks. Clearly however, the approach is fragmented and fraught with conflicts of interest. This should all be compared to the basic premises of effective security which is very much the opposite position of constant monitoring, flagging of issues for acceleration and responding effectively in a rapid and coordinated manner. This is a fundamental and problematic dynamic that is not addressed in the paper.

The Australian security agencies are outside of this commercial structure and laws are constantly under review to enable lawful interception and other functions to be in place so that those agencies can in fact gain a snapshot of what is happening in regards to specific matters, once a warrant is in place. The timescales involved in industry consultation, defining legislation, and designing and installing equipment are significantly out of proportion to the timescales at which new technical and strategic threats can develop out of Internet application and network features. The very existence of this paper and the large set of revisions is indicative of that problem. This is a fundamental and problematic dynamic that is not addressed in the paper.

It is the submitters view that the measures proposed in the paper are reasonable and supportable in the current circumstances, but that the government needs to 'fix' the fundamental problems raised above.

1) The operation of the Internet Protocol layer (the end to end layer) in Australia should be in the hands of a single entity, either government owned or government mandated (ala NBN), and Internet Service Providers should be moved into the market of solely adding value above that basic commodity layer. This will remove the mesh of responsibilities that exist today, and the problematic performance, security, reliability and process issues that such a fragmented approach inevitably brings.

2) International borders should be operated by the Federal Government and features added on an ongoing basis, and without the need for legislation, for the defence of the Australian community. These borders should continue to employ commercial equipment but provide the Government with direct conversations and expertise from equipment providers as regards to hardware and software capabilities, trade-offs and

security requirements as regards protocol and packet monitoring, interception, modification, tracking, recording and blocking.

3) Security agencies should have direct involvement in the operation of these networks and direct involved in the standardisation processes in the IETF and other bodies to ensure that national security features and weaknesses are more fully captured in the development of the technology.

4) The current system of warrant based access to, and examination of, activities and data should still continue in such a Nationally focused Internet model, to ensure that the rights of citizens are protected, and judicial oversight remains in place.

5) The direct involvement of Government agencies should be accompanied by open publication and review of security capabilities and operations so that Internet users can feel comfortable of what is being done in their defence and their name.

These will be initially seen to be extra-ordinary changes. They are however inevitable over time because of the fundamentals identified. The Chinese Government uses such a model for the practical reason that it is in fact the only way to provide deep control and visibility of the Internet. That the Chinese Government lacks oversight and uses such capabilities in undemocratic ways should not undermine Australian Government resolve and it should instead move towards this model with haste. Whilst the capabilities need to be there, it is how they are used that is of concern to the community. If used to protect us over time, then as with all such security functions of the Government, the community will be supportive.

Stakeholder Issues

a) The changes should be supported by the Internet Providers. Firstly, they can continue to make money where it is most effectively made, on the underlying provision of network links, the applications above the internet layer and for the operation and interconnect of enterprise sites and IP-VPNs. This model also firmly identifies and separates out national security and legal responsibilities as regards packet based carriage. They will then see that, over time, as the need for deeper and ubiquitous security functions grows, then so the cost burden as regards equipment, procedures and liabilities regarding packet carriage grows for a layer of their operations that is a commodity function with little opportunity for value-add or differentiation.

b) The changes will be supported by the Security Agencies. They are presently locked out of, or at best at arms length from, this strategically critical infrastructure and security functions whereas they can traditionally tap-into every phone call and monitor any radio band. Yet it is the Internet that today provides a much more powerful avenue for strategic attacks on the Australian infrastructure, and on connected individuals and organisations.

c) The changes will be supported by the community for a number of reasons. Firstly, they are well aware of the poor consequences of the current system in the disjointed way Internet attacks are mediated. Secondly, the community fully recognises the importance of the stability of this infrastructure and the need for appropriate agency involvement. The above of course all critically depend on Government openness and appropriate use of the new capabilities.

d) The changes will be supported by the application and content providers and Internet users for three main reasons unrelated to security.

> i) Firstly, a single national Internet will come at a significant reduction in cost to users due to the elimination of small duplicated access / core links and routers operated presently in the same locations, by each Internet provider for its portion of the Australian user base, and by the elimination of multiple commercial entities and associated business and operational functions for designing, provisioning monitoring and repairing each provider network.
>
> ii) Such a consolidated network will greatly outperform today’s federated networks because large

links provide significant reductions in packet latency, significant improvements in statistical multiplexing gain and more consistence end to end delay and bandwidth characteristics. In contrast, one customer with a small ISP over a slow link affects the performance of a user on a large link with a big ISP when they are interconnected.

iii) A single national network will be able to provide optimal routing stability and optimal packet paths which are impossible in today's Australian infrastructure. For example, in a single network a packet between neighbouring properties will only need to reach the first Internet router before being turned back to that neighbour. In today's model, those two neighbours can be with different providers and their packets face a tortuous delay and packet path across and between two competing provider networks.

iv) A single network infrastructure will enable an orderly and efficient distribution of content and application servers to be deployed by service providers across Australia. The current fragmented approach leads to for example, Internet voice calls being switched in a single city for all national users rather than having a set of switches in each city or location. It also ensures that all content is accessible to all internet users under the same terms rather than the damaging ant-competitive effects of network providers today being able to lock-in content to their networks to the detriment of users of other providers.

v) A secure Internet with increased monitoring and interception will provide better protection for server and users and increase the commercial opportunities and value of those opportunities so growing the addressable market and the size of the customer base, as well as reducing need for financial redress due to security / unlawful issues.

Conclusion

I fully support the Government efforts to undertake the current incremental amendments to various acts and procedures to better enable security functions to be undertaken on the Australian Internet. I have however identified at least two fundamental dynamics that indicate that a wholesale change to the Australian Internet model is required to properly provide in a timely manner, meaningful and fully-functional security capabilities. In support of that wholesale change, I have identified a number of reasons why such a change would be beneficial and supported by a number of stakeholders in the Australian Community.

Alan William O'Neill