INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

17 November 2023

To the Committee Secretary
Environment and Communications References Committee

PO Box 6100
Parliament House
Canberra ACT 2600

By submission: https://www.aph.gov.au/Parliamentary_Business/Committees/OnlineSubmission

RE: Inquiry into the Optus Network Outage

INTRODUCTION

Thank you for the opportunity to contribute to the Senate Inquiry into the recent Optus Network Outage (**Inquiry**).

The Internet Association of Australia's (**IAA**) is a member-based, not-for-profit association representing Australia's Internet community, committed to a better Internet for Australia. Our membership is largely comprised of small to medium sized Internet Service Providers. Our response is primarily for the general public good of the industry.

From the outset, IAA and our members recognise the increasingly important role that the Internet and telecommunications play in our daily lives. To that end, we encourage best practices to be adopted by all industry players, and that government systems and processes should also reflect best practices to ensure that Australians have access to communications.

However, we also acknowledge that the Internet is fundamentally what is known as a 'best effort' network. The protocols that exist are generally highly reliable, but we believe that it is important to recognise and expect they are not designed, nor is the technology capable of being, a completely reliable system with 100% uptime. Thus, it is essential that failure be taken into account, and designed for, when constructing and supplying services that require very high availability. We believe this should be taken into account not only by the telecommunications industry, but also government and other organisations – particularly those providing essential services – in their network design to ensure that Australians will have at all times the means to access essential services, even in the case of a network outage suffered by one carrier.

In addition, we are concerned that this outage may result in a hasty legislative response from government. Although we recognise the serious consequences of the network outage, including landlines on the Optus network unable to make emergency calls, we emphasise that this incident

should not be used to roll in new telecommunications regulations that have not been thoroughly assessed for effectiveness and efficiency. Any additional requirement for 'gold-plated' networks will have to be paid for, and ultimately this will come from consumers themselves.

We understand that this Inquiry primarily focuses on the impact of, and the steps taken, by various bodies in response to the outage, more so than the cause or nature of the outage itself. However, in assessing the impact and flow-on consequences of the outage, we have identified many areas requiring improvement, with regards to both Optus and government, that cannot be divorced from the actual design of networks. Thus, our response primarily offers technical explanations and expectations with regards to network design and outage response.

OUR RESPONSE

a. COMMUNICATION FROM OPTUS TO AFFECTED CUSTOMERS

Industry best practice is to provide updates via the provider's own website (typically listing or mapping affected coverage areas), email distribution lists or SMS alerts to affected customers. Integration between network management and monitoring systems may also exist between the provider and specific customers to provide direct alerts.

We understand that given the circumstances, using these methods to communicate with affected customers may not have been possible either due to the customer's handset, network or access links being down or that Optus may have been unable to reach its own website. Given Optus' scale, however, it is not unreasonable to expect that Optus' own website may be provided, or at least replicated via a third-party content distribution network that would have been operating during the outage.

Of greater concern is that Optus may not have had sufficient information to gauge its own network availability and performance and therefore was unable to provide service availability information. Industry best practice is to continuously monitor the performance of network elements through a separate 'out-of-band' network that operates completely independently to the network Optus uses to provide services to customers. This same out-of-band network should be used to gather logs for diagnostic purposes. In addition to a completely separate out-of-band network, this system should be further supplemented by a system to monitor the monitoring system from a network external to Optus altogether.

We view that the outage affecting all services, thereby restricting communications to affected customers to provide explanations or updates during the outage, highlights flawed design on a number of levels. Optus failed to protect critical parts of its network, failed to have adequate monitoring and management systems in place, and did not have reliable mechanisms to report the outage to customers able to access third party networks.

b. STEPS THAT OPTUS IS TAKING TO ENSURE THAT THIS DOES NOT HAPPEN AGAIN

We note that explanations provided thus far about steps that Optus is taking to ensure that this level of outage will not recur have been vague. We understand that it may take time for Optus to complete its investigations before Optus has a full understanding of the outage. Such an investigation must encompass the triggers, the propagation mechanisms, and the reasons behind the delay in rectifying the problems that occurred, ie the likely flaws in Optus' approaches to remediating the outage and restoring services. We also consider that the explanation provided about the trigger of the initial failure has not been sufficiently clear or comprehensive. Very limited explanation has been given of what Optus and its outsourcing partners did in response to the failure, other than sending people to physically reboot routing equipment. This in turn makes it harder to understand what changes to monitoring and logging, fault escalation, in-country resourcing, and network design are being taken to ensure such an outage does not happen again in the future.

Ultimately, however, we have formed the view that the scale of the outage is the result of not only flaws in the network design and specific equipment configuration, particularly regarding the application of filters, as well as an apparent lack of appropriate network segmentation, but also in Optus' response to the widespread routing failure. It appears that the internet routing table was sent to heavily loaded internal routing equipment – an error that may have been introduced as part of an attempt to restore network services. We expect that Optus will address this by setting appropriate filters and limits and by segregating the external part of the network from the internal one. By ensuring logical separation of the Internet facing network Optus will ensure that an outage of this magnitude does not happen again.

Separation of the Internet facing routing domain from the internal routing domain is not, however, the only mechanism to ensure smooth operation, and indeed smooth restoration, when failures occur. Further segmentation of the network is also advisable such that service areas of the network can be contained. Types of segmentation include geographic, application or service specific methods. In this way, for example, the Optus mobile network could have been restored to service such that calls between Optus mobiles would have been possible. Consumer internet and fixed-line telephony services may have been able to be restored on a region by region basis, enabling access to internal Optus services such as the website or internal calling, prior to re-enabling larger scale inter-connection, and finally global internet connectivity.

However, given the broader impact of the outage on other services, including essential services such as hospital and transport networks, we emphasise that consideration should also be given to encourage government and other service providers to take steps to ensure that a telecommunications outage experienced by one carrier will not have such a massive impact on other essential services. For example, publicly owned transportation networks should not rely on any single communications provider, and should ensure continued service even in the case of a telecommunications outage of its main provider by adopting a redundant provider strategy. This may include internal service provision as well as multiple external providers.

c. COMPENSATION OFFERED TO AFFECTED CUSTOMERS

The role of the Telecommunications Industry Ombudsman and its compensation scheme

We understand that the Telecommunications Industry Ombudsman (**TIO**) can direct telecommunications providers to pay up to $100,000 in compensation for claims brought to the TIO for financial loss caused by a provider's breach of its obligation to a customer. Where it is more suitable for a tribunal or a court to consider a claim, the TIO may choose not to handle a customer's complaint.

We view that the matters that the TIO can consider as 'out of pocket expenses' and 'lost profit' is appropriate, and changes should not be made to allow the TIO to consider claims for compensation on the basis of penalising a provider.

Ultimately, the TIO is an arbitration body, and this role should be kept distinct from that of a regulator.

d. ROLE OF GOVERNMENT IN ENSURING AUSTRALIANS HAVE RELIABLE ACCESS TO TELECOMMUNICATIONS TECHNOLOGY

As our dependence on telecommunications increases in society, its reliability is paramount to everyday life. Indeed, it has become subject to the critical infrastructure regime, with government recognising its role in the Australian economy and society.

We note that as a result, there has been an overwhelmingly large amount of legislation regulating the sector, many of which pertain to security. IAA recognises the role that legislation can play in establishing baseline standards for network reliability and processes that may be helpful in times of crises, whether it be a cyberattack or a network outage. However, we raise our concern that the influx of legislative reforms have been unable to prevent or mitigate the impact of either this outage, or the cyberattacks experienced by both Optus and Telstra in late 2022.

For a number of years, the telecommunications sector has raised the lack of genuine engagement in the development of these legislated instruments, and have warned of the ineffective or impractical nature of such legislation if not developed with adequate consultation with industry. Indeed, the recent June 2022 ANAO Report[1] into the administration of critical infrastructure policy noted the lack of sector specific engagement strategies that the Department of Home Affairs' embarked on in developing the critical infrastructure legislation, as well as an absence of targets supported by a verifiable method to measure performance, and the lack of detail on how performance against the Department's standards contributed to achieving their purpose.

Therefore, we take this as an opportunity to urge the government to work closely with the telecommunications sector in developing legislative frameworks that work practically and are technically feasible or beneficial. We also strongly urge against using this outage as a reason to hastily introduce new legislation without undergoing necessary consultation in a genuine and meaningful manner that ensures the development of a legislative framework that will actually

[1] https://www.anao.gov.au/sites/default/files/Auditor-General_Report_2021-22_38.pdf

ensure better reliability and security. Noting that the Minister for Home Affairs has already mentioned the introduction of new, 'tougher' laws for the telecommunications sector, we note that any legislation that comes into place should pay heed to principles of good policy including proportionality, practicality and effectiveness. We strongly believe that implementing new, reactive legislation will not bring about the intended outcomes.

e. STEPS TAKEN BY THE FEDERAL GOVERNMENT TO ENSURE ACCESS TO ESSENTIAL SERVICES

As noted above, the Internet is fundamentally a best effort network and although generally highly reliable, it is not designed to be 100% failproof. Government should therefore take this into consideration when designing its systems, and should be advising such to other essential services providers in the private and public sector. While the level of redundancy in service provision will remain a business decision, total reliance on one provider's network for any service requiring 100% uptime, is bad design and government should be looking at using disparate technology (such as fixed line and mobile), and possibly multiple underlying networks for network redundancy.

For example, IAA utilises two different carriers for our out-of-band management. Out-of-band management is used to directly access control and configuration interfaces of our network equipment via a secondary interface that is completely physically and logically separate from the primary network connection, to ensure access at all times.

Another measure that should be taken up by both government, and other essential services providers is to connect to Internet exchange peering points, preferably in more than 1 location, and potentially more than 1 provider to ensure widespread availability of its networks.

Government should also have alternative contact arrangements for its affected services, and there should be communication with Australians about those alternative arrangements.

A policy area relevant for government may be to participate in is IETF Standards Making. During the recent outage, although customers on Optus' mobile network were still able to make emergency calls to 000, due to the nature of the fixed line standard, this was not the case for customers on fixed line services. The issue with fixed line services is that when the cabled network fails, many customers have automatic re-connection via fail over to the mobile data network, however, in this case, the Optus mobile network had also lost service. Unlike the mobile emergency related standards where calls to 000 are made possible via connecting to other carrier networks nearby, this is not the case with fixed line networks. We believe this to be an industry wide problem, not isolated to Australia, and the result of a lack of fail over inherent in the technical Standards. Thus, we encourage the Australian government to be involved in IETF Standards Making to ensure that Australians will be able to reach emergency services, even in cases of a network outage, regardless of what service they are using. Either way, if government considers it essential that fixed line services be able to fail over to either mobile or other fixed line networks (given the common transport over the NBN), then this is a technology capability that is fundamentally lacking.

g. OTHER RELATED MATTERS

We also take this opportunity to raise awareness about the below initiatives that should be taken up by government, and also encouraged by government to be taken up by other private sector entities, particularly in the provision of essential services:

- **Resource Public Key Infrastructure (RPKI)**: framework designed to secure Internet routing, and minimise the threat of network hijacking
- **Mutually Agreed Norms for Routing Security (MANRS)**: initiative to implement crucial measures to reduce the most common routing threats
- **Internet Protocol version 6 (IPv6)**: IPv6 has integrated security features and Internet Engineering Task Force built into its design

While these do not directly relate to the recent network outage, they are key initiatives that demonstrate network best practice. The recent outage has demonstrated shortcomings in the network implementations in government and other organisations. As telecommunications become more integral to daily lives, it is important that network best practice is taken up more broadly, and not just within the telecommunications sector.

Therefore, not only are these infrastructure initiatives that should be adopted by government itself to improve the security of government networks, but the government should also work with industry to support the wider deployment of these measures across Australia.

The Asia Pacific Network Information Centre (**APNIC**), the regional Internet registry for the Asia-Pacific region, hosts regular training sessions and forums to support the deployment of these mechanisms in the region.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the Inquiry into the Optus Network Outage. IAA and our members recognise the great importance of telecommunications to everyday lives of Australians, and more broadly, to the smooth operation of our economy and society. To that end, we are committed to ensuring more robust and reliable networks. In order to achieve this, we believe there is a shared responsibility across the telecommunications industry, government, and other sectors to adopt network best practices. We also believe that any legislation introduced to mitigate the risk of such an outage occurring again should be designed in a way that is measured, practicable and effective. We look forward to continuing to work with all stakeholders to ensure this.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (**IAA**) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to corporate and affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark

Chief Executive Officer
Internet Association of Australia