Cyber Security, Triple Zero, and Natural Disasters: What Does Australian Law Say About Telecoms Outages and Network Resilience?

Authors: Thomas Jones (Partner), **Matthew Bovaird** (Special Counsel) and **Patrick Cordwell** (Associate), Bird & Bird

The Singtel Optus Pty Ltd (**Optus**) network outage of 8 November 2023 was a firm reminder of the critical role that telecommunications services have in our interconnected economy. More than 10 million customers were left without access to both fixed and mobile services, and reports abound of effects on public transport, businesses and emergency calling.

While network disruptions happen from time to time, the unprecedented scale of Optus's outage has brought into focus the role of Australia's telecommunications regulatory framework in circumstances where the availability of telecommunications services is significantly impaired. This article examines some key measures under Australian law that are designed to improve network resilience and mitigate the impact of outages. This article also considers a number of prospective regulatory reforms that have been the subject of attention following the Optus outage.

Protecting telco networks against cyber attacks

Telecommunications outages can be caused by one (or more) of a range of different factors at any layer of the network. This is truer than ever, as networks are becoming increasingly complex with more points of potential failure. Nonetheless, many of the possible explanations for an outage are relatively innocent: it could be caused by a power failure, a hardware or software fault, or perhaps simple human error (or a combination thereof).

On the other hand, it is increasingly plausible that a cyber attack executed by a malicious actor could bring a network to its knees. Indeed the Australian Signals Directorate's 2022-2023 Cyber Threat Report identifies that Australia's critical infrastructure is being targeted through attacks against operational technology systems. Given that so much other critical infrastructure relies on network connectivity, telecommunications infrastructure is a particularly significant target for cyber attacks (for example, at the time of writing, a major cyber attack has disabled the network of Ukraine's biggest mobile network operator, Kyivstar, with wide-ranging effects in the context of the country's war with Russia).

It was for this reason that Australia's critical infrastructure regime was expanded by the Commonwealth Government in 2022 to capture assets in the telecommunications sector. This was achieved by the registration of two legislative instruments that require carriers and carriage service providers (**C/CSPs**) to:

- provide the Department of Home Affairs with certain information about assets under their ownership or control; and
- notify cyber security incidents that have an impact on assets to the Australian Signals Directorate within certain timeframes.

The positive security obligations under these instruments broadly mirror those that apply to other classes of critical infrastructure assets under the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**). While the communications sector and related critical telecommunications assets were added to the SOCI Act as part of amendments in 2021, the SOCI Act obligations were originally not "switched on" for telecommunications. The introduction of the parallel telco-specific regime was intended to avoid regulatory duplication by keeping C/CSPs within the regulatory ambit of the *Telecommunications Act 1997* and the existing sector-specific security obligations that are contained in Part 14 of that legislation.

However, in the wake of the Optus network outage and following several other high profile cyber security incidents, the Commonwealth Government has announced that it will now move to bring telecommunications providers within the scope of the SOCI Act. The Government's intentions in that respect are outlined in "Shield 4" of the recently released 2023-2030 Australian Cyber Security Strategy.

It appears that the Government is prepared to take its time rather than rushing through any amendments to the SOCI Act, as it has launched a consultation to extend the sunset of the current instruments from January 2024 to July 2025.

Aligning telecommunications providers to the same standards as other critical infrastructure entities will reduce complexity, particularly for entities that operate within multiple critical infrastructure sectors. However, the shift will not be without challenge for C/CSPs, many of whom undertook a significant amount of work during the past 12 months to bring themselves into compliance with the instruments introduced by the Minister in 2022.

For example, C/CSPs should be aware that in comparison to the existing instruments, the SOCI Act (in its current form) would impose more comprehensive positive security obligations on C/CSPs, including the preparation of critical infrastructure risk management program (commonly referred to as **CIRMP**s). As part of a CIRMP, entities are required to establish and maintain a process to comply with one of the cyber security frameworks or standards specified in the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023* (Cth). Government has indicated that it is already working with industry to design a bespoke CIRMP for C/CSPs.

The proposed shift may also increase the regulatory burden on third party suppliers of hardware and software in the

telecommunications sector. Unlike the instruments, under which asset reporting obligations only apply to C/CSPs, the SOCI Act imposes reporting obligations on all entities that hold a direct interest in a critical infrastructure asset. Companies that manage or control (or that can otherwise influence) a critical telecommunications asset that is owned or operated by a C/CSP may soon find themselves subject to obligations under the SOCI Act. Likewise, companies that provide data storage or processing services to C/CSPs may also be captured.

It is unclear at this stage whether the SOCI Act obligations will supplement or replace existing cyber security obligations under Part 14 of the *Telecommunications Act 1997,* which is commonly referred to as the *Telecommunications Sector Security Reforms* or 'TSSR'. In particular, s 313(1A) already requires C/CSPs to "do their best" to protect their networks and facilities from unauthorised access or interference to ensure both the confidentiality of communications and the availability and integrity of networks and facilities. However, in comparison to the CIRMP rules, the TSSR does not prescribe compliance with a specific cyber security framework or standard.

The existence of the TSSR's security obligation had, up to now, been widely considered to negate the need to bring C/CSPs within the scope of the full suite of cyber security obligations under the SOCI Act. However, the Government's announcement is a clear indication that attitudes on the appropriate level of cyber security regulation have shifted.

Regulating against other threats to network resilience

The Government will be hoping that the TSSR and any future changes to Australia's critical infrastructure framework may prove to be effective in uplifting cyber security in the telecommunications sector, helping to improve network resilience by protecting telecommunications assets against the threat of cyber attacks. However, there remains a question about whether the broader regulatory framework can (and if so, whether it should) impose obligations to protect against risks to network resilience other than cyber attacks. In that regard, it may be helpful to look at regulatory practices adopted overseas.

In particular, the UK's *Communications Act 2003* provides a useful point of comparison. Section 105A(1) of that legislation includes a requirement that providers take appropriate measures to identify the risks of security compromises, reduce the risks of those security compromises, and prepare for their occurrence. This provision is ostensibly comparable to the s 313(1A) 'best efforts' obligation under the TSSR in the *Telecommunications Act 1997*, although perhaps less stringent.

However, the UK Act defines 'security compromise' to include '*anything that compromises the availability, performance, or functionality*' of networks and services, and '*anything that causes signals conveyed by means of the network or service to be lost*'. This means that while the Australian regulatory obligation only requires C/CSPs to protect against threats caused by unauthorised access or interference, the UK regime requires providers to protect against a broad range of other impacts that may affect the resilience of networks and services. The UK telecommunications regulator, Ofcom, has recently published draft resilience guidance in relation to this broad security obligation. Among other things, the proposed guidance requires providers to make sure that networks are designed to avoid or reduce single points of failure.

The Canadian telecommunications regulator's response to the Rogers outage in 2022 also provides an interesting case study, particularly given that the technical circumstances giving rise to that outage were seemingly almost identical to Optus's outage. An interim directive issued by the CTRC now requires carriers that experience any 'major service outage' to submit a report within 14 days detailing plans that have been put in place to prevent similar outages in the future. The report must also record the cause of the outage, steps taken to resolve it and how emergency and accessibility services were affected.

The rules adopted in the UK and Canada reflect growing consensus regarding the importance of telecommunications access, and the consequent need for additional regulatory measures to improve network reliability and resilience and to mitigate the impact of outages.

In the Australian context, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (**DITRDCA**) has launched an inquiry in response to the Optus outage that will report on and make recommendations on issues including resilience and interdependencies between telecommunications networks. Meanwhile, the Senate's Environment and Communications References Committee has also commenced an inquiry that, among other things, is considering the role of government in ensuring that Australians have reliable access to telecommunications services. Given the wide-ranging effects of the Optus outage, it is reasonably likely that these reviews will provide a platform for calls to adopt measures similar to those that are in place in the UK and Canada. At the very least, we expect that the bespoke telecommunications CIRMP obligation under the SOCI Act foreshadowed by the government will require C/CSPs to adopt an 'all hazards' approach to identifying and mitigating hazards that may affect the availability of telecommunications assets.

Access to Triple Zero emergency calling during an outage

While the Australian regulatory framework does not include any broad obligations in respect of the resilience of individual networks, it does include certain rules designed to reduce the impact of outages and maintain the integrity of service access, particularly with respect to emergency calling.

The provision of emergency calling services during outages is regulated by the *Telecommunications (Emergency Call Service) Determination 2019* (**ECS Determination**), a determination made by the Australian Communications and Media Authority (**ACMA**) under Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (**TCPSS Act**).

The ECS Determination imposes rules on C/CSPs regarding the carriage and handling of emergency calls. Key

obligations in relation to emergency calling and network availability include the following:

CSPs that supply a mobile or standard telephone services must provide their end-users with access to the emergency call service if the end-user calls 000 and (where an end-user calls through a mobile service) 112. The CSP must ensure that the emergency call is carried either on their network or by another telecommunications network.

C/CSPs must maintain, as far as is practicable, the proper and effective functioning of their networks and facilities that are used for the carriage of emergency calls to the emergency call service. They must also ensure that their networks have diversity and redundancy.

C/CSPs must have arrangements in place with other C/CSPs to carry emergency calls using their networks and facilities in circumstances where the first C/CSP is unable to carry the calls.

In the event of a significant network outage, CSPs are generally required to undertake welfare checks on any end-users who made an unsuccessful emergency call during the outage.

Non-compliance with the requirements of the ECS Determination contravenes the TCPSS Act and may be subject to enforcement action by the ACMA under the *Telecommunications Act 1997*.

C/CSPs therefore need to make sure that they have arrangements in place to comply with their emergency calling obligations, including in circumstances where networks are degraded or out of action altogether.

The DITRDCA's inquiry will report on and make recommendations on points including the technical and regulatory settings required to ensure the continued access to Triple Zero by users whose network is experiencing outages.

Natural disasters and roaming during an emergency

The Optus outage has also coincided with the recent release of the Australian Competition and Consumer Commission's (**ACCC**) Final Report from its Regional Mobile Infrastructure Inquiry (**Report**). Among other issues, the Report examines the feasibility of temporary mobile roaming during natural disasters or other emergencies.

The Report cites concerns around end users losing connectivity during natural disasters because of damage to network equipment, for example as a result of bushfire or flood, which will occur with increasing regularity as the number and severity of climate change-induced natural disasters grows. While emergency calls must be carried to 000 using the network of another carrier in those circumstances (as discussed above), there is currently no ability for an end user's device to roam onto a surviving mobile network operated by a different carrier for non-emergency communications. The Report found that temporary mobile roaming during natural disasters is technically feasible, though Government agencies and industry would need to develop frameworks to resolve technical and commercial complexities prior to its implementation. The telecommunications regulatory framework will also need to be considered, including potential impacts on competition.

The Commonwealth Government has instructed the Department of Infrastructure, Transport, Regional Development, Communications and the Arts and the National Emergency Management Agency to progress work in designing and developing a mobile roaming capability, reporting back to the Government in March 2024.

We expect that any proposed rules or regulations to implement emergency roaming will be subject to industry consultation in due course.

Applicable consumer protections

The effects of the Optus outage also highlighted the economic importance of telecommunications networks in our interconnected society. In the days and weeks following the outage, the financial costs suffered by businesses were widely reported in the media.

In that regard, C/CSPs need to consider how service disruptions may impact their obligations to retail and small business consumers under Australian law. In particular, the Australian Consumer Law (**ACL**) includes certain consumer guarantees that cannot be excluded by the terms of customer contracts.

CSPs may face some risk of liability under the ACL, particularly if an outage is severe and/or lengthy. The remedy that a consumer is entitled to will depend on the nature of the issue and the specific consumer guarantee that has been breached, but may include refunds, compensation, or contract termination.

A number of other service guarantees are imposed by the TCPSS Act in relation to certain services that are covered by the *Customer Service Guarantee Standard* (**CSG Standard**).

Consumer complaints, including complaints about breaches of the ACL or CSG Standard, are handled by the Telecommunication Industry Ombudsman (**TIO**) under the TIO scheme. The TCPSS Act requires that all carriers and eligible CSPs join and comply with the TIO scheme.

The Senate inquiry into the Optus outage is examining the compensation offered by Optus and the role of the TIO and its compensation scheme, while the DITRDCA's review is also considering the adequacy of how customer complaints processes and compensation processes performed for consumer and small business.

Conclusion

Australia's telecommunications regulatory framework imposes a number of obligations on C/CSPs in relation to the availability of telecommunications networks and services, and how they must respond during outages where service access is impaired. However, the extent to which these rules adequately ensure network resilience and mitigate the impact of outages is under scrutiny following the widely felt effects of Optus's network outage. It is likely that some of the proposed reforms discussed in this article will be implemented during 2024.