Patrick Fair ASSOCIATES

UPDATE

New Cyber Security Consultation, Consumer Data Rights for the Telco sector and other notable developments

1. New cyber security consultation

On 16 July 2021 the Department of Home affairs published a consultation paper titled ***Strengthening Australia's Cyber Security Regulations and Incentives***. The paper states that "Current laws do not provide sufficient clarity regarding cyber security expectations" and "Cross-sectoral cybers security laws lave limited coverage"[1] and proposes new regulations and government activities intended to improve cyber security standards in the private sector.

The paper asks for views regarding the following proposals:

1. Voluntary or compulsory governance standard for large businesses. The paper indicates a preference for a voluntary standard "co-designed" by industry and government.
2. Voluntary or compulsory responsible disclosure policies (**RDP**). The paper requests feedback on the proposed contents of an RDP and lists the potential benefits as a "cost effective way for business to find and address vulnerabilities in software and systems", financial and other benefits to security researchers, and access to better and more reliable products and services for consumers.
3. A security code of practice made under the Privacy Act to impose enforceable minimum (not best practice) standards for the keeping of personal information.
4. A security standard for smart devices where "smart device" means "products that are given extra functionality to connect to the internet". The proposal is to mandate ETSI EN 303 645 or its "top 3 requirements". However, the top 3 requirements are not listed. The first 3 requirements in the standard are no universal default passwords, a means to manage reports of vulnerabilities and a requirement to keep software updated. Interestingly a number of others could also be regarded as "top 3" including." communicate securely", "ensure software integrity" and "ensure personal data is secure"
5. A labelling scheme to indicate and certify cybersecurity compliance of IoT devices. The paper considers a security labelling system co-designed with industry whereby smart devices are given a star rating but seems to prefer a mandatory expiry date labelling system giving the example of a label that says "Cyber protection until 2024"[2]. The paper does not explain how it might be reasonable to label any product as having "cyber protection" or how an expiry date for cyber protection could be realistically estimated.
6. Cyber security health checks for small business. The paper proposes the government offer a review of supply chain risk for small business on a cost recovery basis with successful completion of the review resulting in the right to use a trust mark.[3]
7. New legal remedies for consumers. The paper describes challenges that consumers may face in enforcing consumer guarantees as a remedy for a cyber breach and reports that work is progressing on a regulatory impact statement on the introduction of "civil prohibition …for failing to provide a consumer guarantee as a remedy" and that Treasury will consult with state and

[1] See "Clarity" and "Coverage" in the table on page 15.
[2] See figure 2 page 39.
[3] See figure 4 on page 48.

territory officials regarding whether there are gaps in the Australian Consumer Law (**ACL**) in its application to digital products. This part of the paper also notes the consultation underway on the Privacy Act including on introduction of a direct right of action for individuals that suffer an unlawful interference with their privacy. Submitters are requested to comment on the application of the ACL to digital product and cybersecurity and the adequacy of these laws.

The discussion paper acknowledges the work underway on expanding coverage and improving risk management (including cyber security) of critical infrastructure. The proposals described in the paper are in addition and of general application. Submissions are due on 27 August 2021

2. Consultation on Consumer Data Rights and the Telecommunications Sector, underway

The Consumer Data Rights (**CDR**) framework creates a class of supplier held customer data that customers can share with approved alternative and value-add service providers on a tightly controlled basis. CDR applies to data about individual and business customers. CDR has been partly implemented in banking and implementation is underway in the energy supply sector. Treasury has commenced the process of rolling out CDR in the Telecommunications sector with a consultation.

In a Strategic Assessment Consultation paper Treasury seeks feedback regarding use cases and datasets which, if included in the CDR framework would improve the consumer experience and/or have other benefits. In a Telecommunications Sectoral Assessment Consultation paper Treasury asks for feedback on a range of matters including who, within the telco sector, should be covered by the scheme, the datasets to be included, how public interest, privacy and confidentiality issues can be managed and how to optimize the scheme. Submissions close on 19 August 2021

3. Other notable developments

3.1. The International Production Orders Bill becomes law

The *Telecommunications Legislation Amendment (international Production Orders) Bill 2020* (see our Update of March 2020) passed both houses on 24 June 2021 and received Royal Assent on 24 July 2021. The Bill was amended to address the recommendations of the Parliamentary Joint Committee on Intelligence and Security and generally became law without a sunrise period.

Interestingly, to be operable the new law requires an international agreement with the government of the country of the recipient or issuer of any International Production Order (**IPO**). The Hon Karen Andrews MP, Minister for Home Affairs, said this in her Second Reading speech on the bill "The passage of this bill is a critical step to finalising a bilateral CLOUD Act agreement with the United States, a longstanding trusted partner and home to many global communications providers, including Apple, Facebook, Google and Microsoft." Accordingly, the issue and receipt of IPOs will not proceed until an international agreement with the USA and/or another country, is finalised.

3.2. Threshold for a consumer transaction is now $100k

On 1 July 2021 any goods or services valued up to $100,000 (up from $40,000) are deemed to be supplied to a consumer and subject to consumer guarantees including in business-to-business transactions. Goods and services valued over $100,000 are subject to consumer guarantees if they are normally bought for personal or household use.

With this in mind, suppliers wishing to limit liability for business-to-business transactions under $100,000 should check that their supply terms include a limitation of liability that complies with the formulation prescribed by the Australian Consumer Law.

Please contact me if you have any questions regarding the matters discussed in this update.

patrick@patrickfair.com **0411361534**