TMT

The Australian Landscape

December 2021

CORRS
CHAMBERS
WESTGARTH

corrs.com.au

Welcome to the fourth edition of *TMT: The Australian Landscape*.

As we emerge from the tumultuous disruption of the COVID-19 pandemic, governments around the world have formed a clearer picture of the level of reliance on, and in turn the vulnerabilities of, digital infrastructure in key industry sectors. Similarly, as the involvement of social media and other online platforms and emerging technologies in the lives of consumers continues to deepen, they are facing increasing regulation from a privacy and human rights perspective. Over the course of this year, the Australian Government has introduced a number of very significant regulatory changes in these areas which warrant careful attention and which we explore in this edition.

Cyber security resilience is a major focus in several areas of new and emerging regulation in Australia. The amendments to the *Security of Critical Infrastructure Act 2018* (Cth) sees it now apply to 11 broadly framed industry sectors and impose new reporting and obligations and extensive government powers in the event of a cyber security incident (these powers going beyond those that other members of the 'Five Eyes' alliance have implemented).

Recognising the prevalence of ransomware attacks, under the Ransomware Payments Bill 2021 (Cth) the Australian Government has also proposed a mandatory reporting obligation where an entity makes a ransomware payment. As we discuss in this edition, navigating the cyber security risks faced by organisations and the increasingly far-reaching regulatory landscape is a significant issue that must clearly be addressed at the boardroom level. 2022–2023 will be a big year for major changes to privacy regulation in Australia. These changes are still subject to consultation but will likely include a number of elements from the GDPR and the CCPA as well as include significantly increased penalties for contravention.

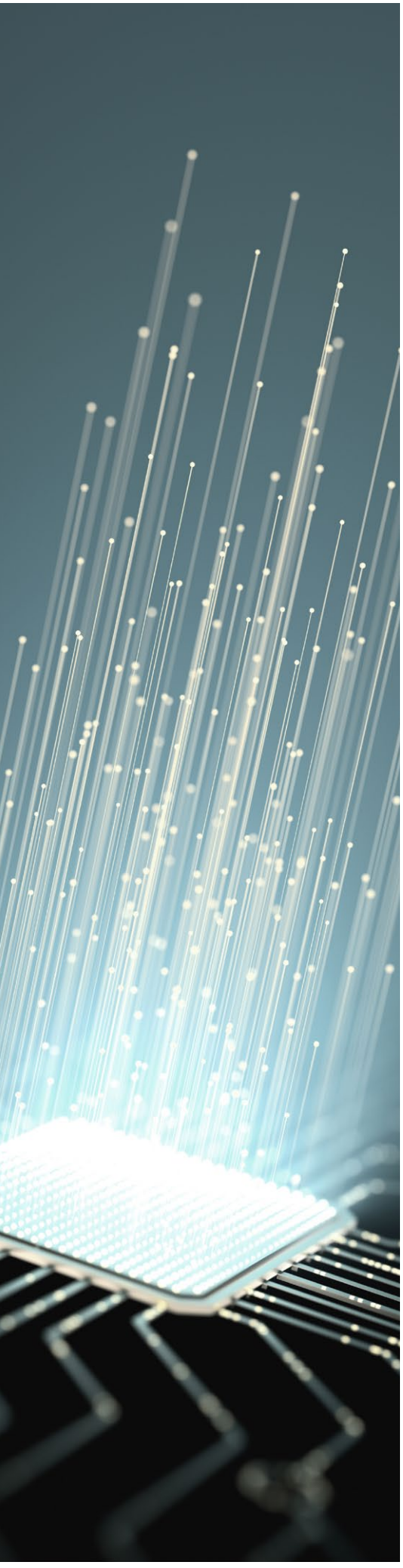
On the other hand, the opportunities in the Australian market are significant for technology companies that can effectively navigate these emerging regulatory regimes, including in the areas of digital identity, artificial intelligence, financial technologies and other technologies identified by the Australian Government as 'critical technologies' in its Action Plan for Critical Technologies.

We hope you enjoy this edition of *TMT: The Australian Landscape*.

Please contact any member of the Corrs TMT team if you wish to discuss any of the issues raised.

James North
Head of Technology, Media and Telecommunications

Frances Wheelahan
Partner



Contents

Ransomware: key legal issues facing organisations under attack

By James North, Head of Technology, Media and Telecommunications, Mark Wilks, Head of Commercial Litigation, Justin Gay, Special Counsel and Rebecca LeBherz, Special Counsel

Ransomware[1] attacks have become more frequent and serious in recent years in line with a steep increase in the overall rate of cybercrime globally.

Targets range from small unlisted companies to large organisations and government agencies, often with sophisticated cyber defences and policies. The past two years have been particularly challenging for organisations due to the rise in remote working and the continued uptick in general and supply chain ransomware attacks.

The Australian Government has announced a number of proposed responses to ransomware attacks, including legislation to mandate the reporting of ransomware payments. There has also been increasing commentary on directors duties with respect to cyberattacks. The Australian Government (along with the US) has expressed great concern about the growing cost to the economy of ransomware attacks and has flagged a strong indication of increased regulation in this space in future.

This article explores the key issues including:

- is it legal under Australian law to pay a ransom;
- the reporting obligations under current Australian law;
- directors duties with respect to ransomware attacks;
- potential regulatory risks and class actions;
- new proposed legislation affecting ransomware payments and reporting; and
- pertinent insurance considerations.

Given the increased risk of ransomware attacks and the strong likelihood of imminent changes to the law in this area, we recommend all organisations keep a close eye on legal developments and, if subject to a ransomware attack, seek urgent legal advice before responding, as the potential legal and reputational risks associated with paying a ransom are significant.

Is it legal in Australia to pay a ransom?

Under Australian law, it is generally not illegal for an organisation to pay a ransom. However, it's complicated and requires careful decision making.

There are specific offences under the *Commonwealth Criminal Code* and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) which make it an offence for payments to be made either for money laundering purposes, or to a 'terrorist organisation' or an organisation proscribed by UN sanctions or Australia's autonomous sanctions.

The criminal offence of money laundering necessarily involves the payment of money in circumstances where the payer has actual knowledge that there is a risk that the money will be used as an instrument of crime, or if the person is reckless or negligent to this risk. Similarly, for the offence of making payments to a terrorist organisation, the offence occurs if the payer is 'knowing or reckless' to the fact that the organisation was proscribed as a 'terrorist organisation'.

An organisation that is considering whether to pay a ransom also needs to carefully consider what it knows about the perpetrator. This can often be discovered via forensic investigations. Questions to ask include:

- Is the perpetrator part of a known criminal outfit or terrorist group? An up-to-date list of 'terrorist organisations' is maintained on the Australian National Security website.
- Is it a state actor?

1 Ransomware attacks involve cybercriminals hacking into an organisation's computing environment and illegally accessing data, or installing malware to seize control of the organisation's computer systems. The cybercriminal demands payment from the organisation of a sizeable ransom to hand back control, often under threat of publicly releasing sensitive data if a ransom payment is not made.

- Is the perpetrator an organisation listed as either a terrorist organisation, or on the UN or Australian sanctions lists?[2] The breach of some sanction lists are strict liability offences so businesses will be held liable even if the breach was not intentional, reckless or negligent.[3]

The answers to these questions will determine whether or not it is legal to pay.

If the perpetrator is unknown, or there is no indication that the perpetrator is a declared terrorist organisation, or part of a criminal body intending further crimes, then payment to the organisation is unlikely to be 'knowing or reckless' so as to constitute an offence.

Reporting obligations under current Australian law

At present, there are no general mandatory reporting obligations applicable to ransomware attacks under Australian law.

In New South Wales, it is an offence to conceal a serious indictable offence where an organisation is in possession of information that will materially assist in apprehending, prosecuting or convicting an offender. Where the identity of a perpetrator is unknown, it is unlikely that a failure to report the attack would in itself make out this offence. However, you should obtain legal advice on your specific circumstances.

Depending on the nature of the organisation, the industry in which it operates, and the particular impact of the ransomware attack, further specific legal reporting obligations may arise, including:

- if the attack involves an unauthorised disclosure of 'personal information' then the organisation may be required by the *Privacy Act 1988* (Cth) (**Privacy Act**) to report the incident to the Office of the Australian Information Commissioner (**OAIC**) as soon as reasonably practicable;
- if the organisation is a regulated financial services entity (such as a bank or superannuation fund) then it may be required under relevant prudential standards such as CPS234 to notify the incident to the Australian Prudential Regulatory Authority (**APRA**) within 24 hours of becoming aware of the incident;
- that the organisation may be required to report a ransom payment to the Australian Transaction Reports and Analysis Centre as a 'suspicious transaction' under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth); and
- under the *Security of Critical Infrastructure Act 2018* (**SOCI Act**), which applies to entities in the electricity, gas, water and ports sectors in Australia, although it is currently being amended by the Commonwealth Government to greatly expand its operation to other sectors deemed to involve the operation of 'critical infrastructure'. If the organisation operates 'critical infrastructure' within the meaning of the SOCI Act then there may be mandatory reporting obligations to report cyber security incidents to the Australian Signals Directorate. Proposed amendments to the SOCI Act would also give the Minister for Home Affairs the power to intervene and potentially direct the organisation on how to respond to a ransomware attack (including whether or not to pay the ransom).

An impacted organisation should also consider whether any notifications are required under any applicable contracts of insurance, or triggered under third party contracts (either under specific data breach notification requirements or other clauses such as confidentiality clauses).

Director duties with respect to ransomware attacks

Company directors and officers have a duty to exercise their powers and discharge their duties with care and diligence.[4] This duty is uncontroversial and is a cornerstone of the directors duties set out in the *Corporations Act 2001* (Cth) (**Corporations Act**). Over the past 20 years, section 180(1) of the Corporations Act has been tested with respect to various circumstances occurring in the course of company management. It is now possible that the duty will apply to ransomware attacks, how boards prepare and protect themselves, and how they respond.

Ransomware risk is by now (or should be) well known to directors and boards and it will become increasingly difficult to argue that the duty of care and diligence does not require directors and boards to consider, at minimum, the foreseeable risk of harm that would be caused by a ransomware attack. They also need to take steps to protect and respond to the reasonable standard set in the Corporations Act.

2 Such as those maintained by DFAT or the UN.

3 *Charter of the United Nations Act 1945* (Cth) section 27(8); *Autonomous Sanctions Act 2011* (Cth) section 16(8).

4 Section 180(1) of the *Corporations Act 2001* (Cth). A director also has a duty to act good faith and in the best interests of the company, but we have focused on the most likely relevant duty, care and diligence.

When determining whether the duty to act with care and diligence has been breached, a court will balance the foreseeable risk of harm to the company against the potential benefits of having addressed the risk. As with more 'traditional' risks, directors that have conducted such a balancing exercise for themselves, and who act based upon a rational and informed assessment of the company's best interests, may have the protection of the 'business judgment' rule.

We are yet to see any significant Australian cases or regulatory prosecutions relating to breaches of directors duties based on ransomware attacks or preparedness. Directors should be aware that the losses caused by a ransomware attack go beyond the ransom paid. Following an attack there can be substantial business interruption expenses and in the case of public companies an immediate sell down in securities and reduction in market value. For example, in November 2020, Isentia, a media intelligence and data company listed on the ASX, experienced a cyber-attack that affected its operations. Isentia spent around up to A$8.5 million on remediation and provide discounts or credits to affected customers, significantly reducing revenues. Isentia's share price was significantly reduced and Isentia shareholders eventually voted in favour of a takeover offer.

Potential regulatory risk and class actions

Regulatory issues

As the risk of cyber-attacks increases, it is highly likely that the OAIC and other government regulators will increase their regulatory action.

The OAIC has the power to seek civil penalties from organisations that have breached the Privacy Act as well as make public determinations that organisations breached privacy laws. The OAIC has already publically called for 'a greater ability to pursue significant privacy risks and systemic non-compliance through regulatory action', including stronger powers to give civil penalties. Under the Privacy Act, affected persons may be able to seek compensation. However, compensation is generally[5] not awarded unless an affected individual supplies evidence of loss or damage.

Recently the OAIC identified that Uber had been approached by unknown persons who had accessed and downloaded personal information, including names, email addresses and mobile phone numbers of users of the Uber app.

After being notified of this breach, Uber paid US$100,000 under a 'bug bounty' program. In the view of the OAIC, rather than identifying the vulnerability and disclosing the breach responsibly, Uber's 'immediate response was to pay the attackers – who had intentionally acquired personal information and exploited a vulnerability to extort funds – under a bug bounty program'.[6] The OAIC determined that Uber failed to comply with the Australian Privacy Principles. No compensation was awarded for affected persons because under the Privacy Act the Commissioner is not authorised to award compensation simply because an organisation has breached the Act. Given the increasing trend towards increased regulatory action, this may change.

The Australian Securities and Investments Commission (**ASIC**) has already commenced an action alleging that a financial services licensee breached its obligations by failing to take steps to manage cybersecurity risk, which allegedly let to a cyber attacker accessing client information.

There is a global trend of more aggressive enforcement by regulators against businesses that have experienced cyber breaches. In the United States, the Federal Trade Commission (**FTC**) is taking action against businesses that allegedly failed to implement appropriate data protection measures for consumers' personal information. For example, in *FTC v Wyndham Worldwide Corp*[7] it was alleged that inadequate cybersecurity practices had exposed consumer data to unauthorised access and theft.

The FTC sought compensation for affected consumers that would redress the injury resulting from Wyndham's failure to protect personal information. Similarly, the FTC brought an action against Equifax after it was hacked and the personal information of 147 million people was compromised. As part of a settlement with the FTC, Equifax agreed to pay at least US$575 million, and potentially up to US$700 million, to assist the people affected by the data breach.

Class actions

Ransomware class actions have already commenced overseas. An action has commenced against Canon USA Inc after a ransomware attack affected employee information. In the United States, Equifax also settled a class action with 147 million class members that required Equifax pay reimbursement for losses caused by the breach and at least US$1 billion on data security over five years.[8]

The class action regime in Australia would facilitate such actions and these should be expected. The Privacy Act also includes a representative complaint regime, which could feasibly be utilised in a ransomware claim scenario.

5 There have been notable exceptions to this.
6 *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy)* [2021] AICmr 34 (30 June 2021) [125].
7 *FTC v. Wyndham Worldwide Corp* 799 F.3d 236 (3d Cir. 2015).
8 *In re: Equifax, Inc. Customer Data Sec. Breach Litig. (Huang v. Equifax, Inc.)*, 2021 WL 2250845 (11th Cir. June 3 2021, 2021) 6–7.

Proposed legislation affecting ransomware payments

The Ransomware Payments Bill 2021 (Cth) currently before the parliament will introduce mandatory reporting obligations for ransomware payments.

If passed, any entity that makes a ransomware payment will be required at law to give written notice of the payment to the Australian Cyber Security Centre (**ACSC**) as soon as practicable. A civil penalty of 1,000 units (currently A$222,000) will apply to a failure to report.

The Bill proposes that where a notification is made, ACSC can then disclose information (other than personal information) in the notification to:

- any person including the public (in de-identified form) for the purpose of informing about the cyber threat environment; and
- Commonwealth, state or territory agencies for purposes relating to law enforcement.

The Bill was first introduced to the House of Representatives on 21 June 2021 and remains before the lower house at time of writing.

Under proposed amendments to the SOCI Act, the Minister of Home Affairs will have greater oversight of cyber incidents affecting critical infrastructure and a power to issue a direction that the responsible entity for critical infrastructure do, or refrain from doing, a specified act or thing in dealing with an incident.[9] Such a direction could prohibit the payment of a ransom.

Insurance issues

Recent years have seen the emergence of the cyber insurance market, as traditional Directors and Officers (**D&O**) insurance failed to adequately respond to cyber and data risks. Namely, D&O policies provide for defence costs but not cyber remediation costs and do not account for the preventative steps often required in ransomware scenarios.

The Australian cyber market is continuing to grow as boards are increasingly focused on cyber risk management. The market has grown both in respect of higher limits being purchased, and also in the total number of cyber policies placed.

However, the effect of the continued growth in attacks (and therefore claims) is reflected in the market steadily hardening – we have seen increased premiums for risks (15-20% average annual premium increases), capping of policy limits, and insurers requiring more underwriting information before a policy is written.

Whether or not ransomware payments are covered under a cyber insurance policy will depend on the exclusions and scope of the insurance purchased. This should be a further key consideration for an organisation considering its position in response a ransomware attack, and whether or not to pay any ransom.

Looking ahead

The legal issues associated with ransomware attacks need to be navigated carefully, particularly as the law changes and is developed in this area in response to the ever growing risk of ransomware attacks.

9 Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) section 35AQ

A tale of two Bills: reform of Australia's critical infrastructure laws

By James North, Head of Technology, Media and Telecommunications, Philip Catania, Partner, James Wallace, Senior Associate and Jack Matthews, Lawyer

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**SOCI Bill**) has passed Parliament, amending the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**).

The original SOCI Bill has been subject to extensive amendments over the past 12 months as a result of Parliamentary committees and consultation processes which have significantly altered the Parliament's original draft.

A tale of two Bills

Following the PJCIS recommendations, the original SOCI Bill was split into two amendments, Bill One (the SOCI Bill as passed by Parliament) and Bill Two (for which there is no timeframe for passing).

The PJCIS recommended splitting the bill into two to expedite the passing of government powers to address increasing security threats to Australia's critical infrastructure and to enable further industry consultation on new security obligations and sector-specific rules.

Bill One, which will commence imminently, increases the scope of the SOCI Act and introduces new government powers deemed vital for maintaining the security of Australia's critical infrastructure. The key amendments in Bill One include:

- **The expansion of the sectors regulated**. The businesses and industries which fall within the SOCI Act have been significantly expanded. Government no longer deems critical infrastructure to be limited to the original four sectors of electricity, gas, ports and water. The SOCI Act now applies to 11 broadly framed sectors which cover large portions of the economy, including sectors that are not traditionally considered to be infrastructure (for instance, financial services, banks and markets, supermarkets, data storage or processing, communications, education and transport).
- **New reporting and notification obligations**. Responsible entities (i.e. owners and operators of critical infrastructure assets) must notify the Australian Signals Directorate (**ASD**) of cyber security incidents which have a 'significant impact' on an asset within 12 hours. Non-compliance carries civil penalties. A 'significant impact' is an incident which has materially disrupted the availability of essential goods or services provided using the asset (or as otherwise specified in sector-specific rules). All other cyber security incidents must be reported within 72 hours. This will have significant implications for the way cyber security teams conduct investigations and report on cyber incidents.
- **New government response powers**. The SOCI Bill has introduced extensive government powers in responding to cyber security incidents:
  - an **information gathering direction**, requiring a responsible entity to provide information in relation to a cyber security incident (for instance, the impact of the incident on the asset);
  - an **action direction**, whereby the Home Affairs Minister can direct an entity to do, or refrain from doing, any action deemed reasonably necessary, proportionate and technically feasible, but only if the entity is unwilling or unable to resolve a cyber security incident; and
  - **step-in rights** (termed 'intervention requests'), which provide the ASD a 'last resort' power to take control of an asset where an entity is unwilling or unable to resolve a cyber security incident.

In accordance with the PJCIS recommendations, the remainder of the amendments proposed under the original SOCI Bill will be deferred to Bill Two to allow further consultation with industry on the scope of the proposed obligations and potential regulatory overlap. Bill Two is expected to include:

- **New positive security obligations on responsible entities**. These include a requirement to adopt risk management programs for critical infrastructure assets. Some entities have existing security obligations, for instance, APRA-regulated entities are already required to provide risk management declarations in accordance with CPS 220 and undertake systematic testing of information security controls under CPS 234. As such, these proposed amendments have left many regulated entities concerned that they will be subject to multiple cyber security regimes with inconsistent obligations.
- **A regime for the declaration of, and obligations relating to, systems deemed to be of national significance (SONS)**. As currently proposed, responsible entities of SONS will be subject to additional obligations, including maintaining incident response plans, undertaking cyber security exercises and (in some circumstances) allowing the installation of ASD's reporting software.

Key takeaways and next steps – Bill One

Responsible entities of critical infrastructure assets must ensure their cyber security and notification procedures are aligned with the new reporting obligations outlined in the SOCI Bill. Whilst entities in sectors which are currently subject to similar regulations (such as the telecommunications and financial services sectors) may be able to leverage existing cyber security and notification processes, this is a significant regulatory burden for entities in other sectors which are now deemed to be critical infrastructure. Operators of critical assets in industries not previously regulated will need to ensure they put in place appropriate cyber incident monitoring and reporting systems in order to comply.

Generally, the SOCI Bill assumes that all assets and systems of a responsible entity are critical infrastructure assets so as to be subject to the reporting obligations and government powers, unless excluded by the sector specific rules. These sector-specific rules are yet to be released, but are expected to more precisely specify the scope of assets to be captured by the regime. Consequently, the regulatory burden is likely to be high in the short-term, but may be wound back in the future. For instance, 'critical banking assets' are defined to include all assets and systems of an authorised deposit taking institution that are deemed critical to the sector.

Similarly, 'critical telecommunication assets' capture all assets owned by a carriage service provider and used in connection with the supply of carriage services. This lack of refinement means that in many cases, responsible entities will need to assume that the obligations under the SOCI Bill apply to all of their assets and systems (not just those which may ordinarily be considered 'critical').

In some instances, the SOCI Bill goes beyond assets owned by a responsible entity and captures a responsible entity's supply chain, such as cloud storage or data processing providers. Responsible entities will need to review vendor contracts to ensure they contemplate compliance with the new government powers. This may include requiring vendors to provide assistance to responsible entities in responding to directions from the government and the ASD (for instance providing information on a cyber security incident or facilitating access to a critical asset).

The new government response powers go beyond the measures other members of the 'Five Eyes' alliance have implemented. Throughout the SOCI Bill's consultation process, industry consistently voiced concerns with these powers, noting that they posed an additional risk to assets and systems. For instance, if not exercised with extreme caution and the relevant technical expertise, any intervention with an entity's critical assets could have significant, unintended and detrimental ramifications for both the entity and third parties. Following the PJCIS recommendations, the Home Affairs Secretary is now required to provide the PJCIS with reports about incidents in response to which the new government powers have been exercised. However, this may be of little comfort to responsible entities given that there is no prescribed timing for the reporting and judicial review of any government direction or intervention remains unavailable under the SOCI Act.

Key takeaways and next steps – Bill Two

The PJCIS recommended Bill Two be postponed due to the current uncertainty as to the application and requirements of the positive security obligations. The precise requirements were due to be prescribed in 'sector-specific rules', however these are yet to be developed.

It is unclear when Bill Two will be introduced to Parliament, however the Department of Home Affairs has already recommenced the consultation process, hosting a forum with industry to plan next steps. This consultation process presents a further opportunity for industry to gain clarity on the scope of the obligations to be imposed under Bill Two and to align these obligations with existing regulatory frameworks. For example, coordinating the risk management obligations imposed on the communications sector with the requirements already mandated by the Telecommunications Sector Security Reforms.

Organisations should assess the application of the legislation to their business, and if they are considered to be a responsible entity should participate in sector consultations to ensure that their obligations are clear and do not contradict, duplicate or cut across existing regulations.

Cyber in the boardroom: navigating an evolving governance landscape

By Philip Catania, Partner, Kit Lee, Lawyer and Alexander Hender, Lawyer

In light of the increasingly sophisticated cyber threats being faced by many businesses, the Australian Government is planning to introduce a new set of standards to enhance the cyber governance landscape, which are likely to have far-reaching effects on how companies – and their directors – manage cyber security risks.

As the scope of directors' duties broaden and the measures of accountability for cyber security practices sweep into the boardroom, organisations will need to take action to ensure they are in the best possible position to mitigate cyber threats.

In July 2021, the Australian Government released the *Strengthening Australia's cyber security regulations and incentives* discussion paper (**Discussion Paper**) as part of its A$1.67 billion 2020 Cyber Security Strategy.

The Discussion Paper addresses a variety of cyber-related issues, but one key recommendation calls for the introduction of cyber security governance standards (voluntary or mandatory) applying to businesses **not** currently covered by sector-specific cyber governance rules – around two thirds of ASX 200 companies. The Discussion Paper sets out two potential governance standards:

1. Voluntary governance standards for larger businesses describing the responsibilities and processes for managing cyber security risk.
2. Mandatory governance standards which larger businesses would need to comply with in a specific timeframe.

These proposed standards will likely impact the application of the directors' duties under the *Corporations Act 2001* (Cth) (**Corporations Act**) by shaping the scope of reasonable conduct that is expected of directors in respect of cyber security risk. While only presented at a high-level to date, the substance of the standards will be further clarified once the government has considered the public consultation submissions (which closed 27 August 2021).

The cyber governance landscape

There are currently a number of sector-specific regulations which address cyber risks, including:

- the Australian Prudential Regulation Authority's CPS 234, which applies to banks and deposit-taking institutions, and attributes responsibility for a company's information security to the board;
- the *Security of Critical Infrastructure Act 2018,* which establishes a range of 'enhanced cyber security obligations' in respect of critical infrastructure assets; and
- the recent *Ransomware Payments Bill 2021*, which proposes the introduction of mandatory reporting of any ransomware payments to the Australian Cyber Security Centre.

More broadly, the Australian Securities and Investments Commission (**ASIC**) has stated that the directors' duties under the Corporations Act may govern directors' management of a company's cyber risks. However, the Discussion Paper highlights that the existing directors' duties lack the clarity and coverage necessary for enforcement to occur – there are currently no domestic cases where directors' duties have been found to have been breached by cyber security failures.

In particular, the Discussion Paper describes the following factors as contributing to this ineffectiveness:

- the Corporations Act was not originally intended to address cyber security issues;
- the broad scope and principles-based nature of director's duties; and
- directors' duties are focused on protecting the interests of shareholders, rather than customers.

The impact on directors' duties

The introduction of cyber security governance standards (voluntary or mandatory) setting out responsibilities for directors in managing cyber risk would clarify the operation of the directors' duties. For example, section 180 of the Corporations Act provides that directors must exercise their powers and perform their duties with the degree of care and diligence that a reasonable person would exercise if they:

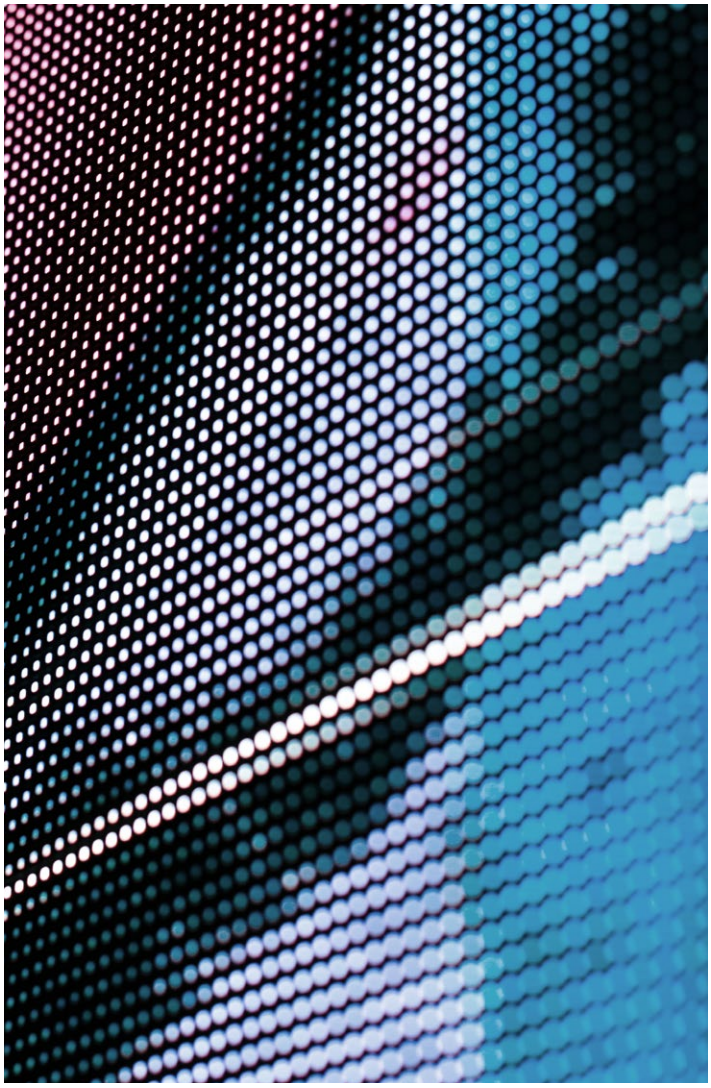
- were a director or officer of a corporation in the corporation's circumstances; and
- occupied the office held by, and had the same responsibilities within the corporation as, the director or officer.

There are minimum standards of care expected of all directors. For example, a director must:

- acquire a basic understanding of the business;
- be continually informed about the activities of the company; and
- generally monitor the business' affairs.

In assessing whether a director has contravened their duty of care, the court will attempt to 'characterise' the director according to the reasonable standard of care – that is, the court will identify what the director ought to have done with reference to existing case law, general industry practice and established standards (such as those described above).

The introduction of the cyber security standards will directly inform the characterisation of the director, and the conduct the director is expected to undertake in complying with their duty of care. According to the Discussion Paper, the standards will assist the court in defining the types of cyber risk failures that will constitute a breach of the directors' duties. Additionally, the standards will likely help to frame and complement the operation of other duties under the Corporations Act such as the corporate disclosure obligations (e.g. where a director fails to disclose a cyber breach likely to impact the value of a company's securities) and the duty to act in the best interests of the company and for a proper purpose.



Looking ahead

It is unclear how the standards will be published and implemented at this stage (i.e. through amending legislation or a separate enforceable standard) and whether an independent regulatory body will be established to manage compliance with the standard. The Discussion Paper notes there is currently no regulatory body with the requisite expertise or resources to administer a mandatory standard for all large businesses.

However, we expect the formulation of the cyber standards to empower ASIC with sharpened tools to better enforce directors' and company officers' management of cyber threats and risks, potentially opening up the suite of liability and enforcement options under the Corporations Act (e.g. civil penalties, disqualification or orders to pay compensation).

While it is not envisaged that the proposed standards will implement specific technical controls, they are likely to have far-reaching effects on the way companies deal with cyber security risks. In particular, the standards will solidify the risk of directors being held liable for breaches of their Corporations Act duties in the event their companies do not have the necessary risk management framework in place to safeguard against cyber threats.

Critical technologies and Australia's defence export control regime

By Frances Wheelahan, Partner and Robert Ceglia, Associate

On 17 November 2021, the Australian Government's Critical Technologies Policy Coordination Office (**CTPCO**) released *The Action Plan for Critical Technologies* (**Action Plan**).

The Action Plan outlined 63 different technologies (which fall broadly within seven categories) that it believes will have a significant impact on Australia's national interest. These technologies include current and emerging technologies such as AI, sensing and navigation technologies, quantum technologies, advanced robotics and autonomous systems and space technologies.

CTPCO's Action Plan highlights the areas in which the Australian Government intends to make focused investment and the types of technology that may be subject to increased regulatory scrutiny.

One of the existing legislative regimes that will likely be key in ensuring there are appropriate controls on these critical technologies is Australia's defence export control regime. While a common misconception is that Australia's defence export control regime only applies to weapons or other technology used by military, the law also regulates many 'dual-use goods' – that is, goods designed for commercial use, but which could also have a military use. The list of 'dual-use' goods is long, and controls can apply to a range of technology, including some commonly used during R&D activities.

With the renewed focus on critical technologies (and severe penalties for businesses who get export compliance wrong), this article provides an overview of the key requirements under the *Defence Trade Controls Act 2012* (Cth) (**DTCA**) and related export control laws.

What is Australia's defence export control regime?

Australia's defence export control regime is made up of several pieces of legislation, including:

- the DTCA; and
- the *Customs (Prohibited Exports) Regulations 1958* (Cth) (**Customs Regulations**).

These laws are supported by Australia's sanctions laws (which prevent exports to specific countries or individuals) and overarching obligations relating to technology with a military end-use or that could be used in a weapons of mass destruction program. The focus of this article is on the DTCA and Customs Regulations as they may impact a broader range of businesses (beyond those that develop military technology).

Together, the DTCA and the Customs Regulations place controls on the tangible and intangible export of 'controlled' goods and technology. Their application is broad, and they can, for example, control activities commonly performed during R&D, such as exporting prototypes for testing or emailing design files to someone located outside Australia (including to a subsidiary, collaborator or business partner).

If it is anticipated that goods or technology might be shared with persons located outside of Australia who are not employed by your company, there are two questions that should be asked to determine if the defence export regime applies:

1. Are the **goods or technology** 'controlled'?
2. Is the **transfer** of goods or technology within the scope of the defence export regime?

If the defence export regime applies, consideration should also be given to whether an exception applies. If not, an export permit may be required to share the goods or technology.

What goods and technology are 'controlled'?

Goods and technology will only be controlled if they meet the parameters for an item in the Defence and Strategic Goods List (**DSGL**). Although the DSGL covers a broad range of goods and technology, only items that meet very specific parameters are controlled.

For example, certain types of telecommunications equipment are controlled under the DSGL if the equipment meets quite specific control thresholds (e.g. it is designed to withstand certain types of radiation or operate at extreme temperatures). Other telecommunications equipment won't be controlled unless the equipment falls within the scope of another DSGL Item.

The DSGL draws an important distinction between goods and technology listed in Part 1 and Part 2 of the DSGL:

- **Part 1** of the DSGL lists munitions and military goods and technology (e.g. firearms). Stricter controls apply to Part 1 goods and technology.
- **Part 2** of the DSGL lists 'dual-use' goods and technology (e.g. computers designed to operate at very high or very low temperatures are listed in Part 2 of the DSGL). There are more exceptions available for Part 2 goods and technology. However, the scope of Part 2 goods and technology is broad, and many items can often be unexpectedly subject to export controls.

Many of the critical technologies identified in CTPCO's Action Plan may fall within the scope (or may do so in the future). For the technologies that do fall within the scope of the DSGL, there is likely to be increased regulatory scrutiny on the export of that technology.

What activities are regulated?

Whether the DTCA or the Customs Regulations apply to a particular situation depends on how goods and technology are proposed to be transferred outside of Australia. In either case, if the activity is controlled, the exporter may require a permit to transfer the goods or technology outside of Australia.

Customs regulations

The Customs Regulations and *Customs Act 1901* (Cth) deal with the export of **tangible** goods – either goods listed on the DSGL or goods that contain intangible technology within the scope of the DSGL (**DSGL Technology**) (e.g. a USB containing information on how to fabricate goods listed on the DSGL).

These exports occur commonly when a person exports a prototype for testing, or takes a USB or laptop containing DSGL Technology to a country outside of Australia.

DTCA

The DTCA predominantly deals with transfers of **intangible** technology (i.e. DSGL Technology). There are three activities controlled under the DTCA:

1. Supply. The first (and most frequent) activity controlled under the DTCA is the **supply** of DSGL Technology. This occurs when a person in Australia provides DSGL Technology to another person located outside of Australia (including providing access to that technology).

   A supply commonly occurs when conducting R&D or when sharing information overseas including DSGL Technology. Supply includes an individual sending an email to someone overseas, or providing another person with access to a cloud based platform containing DSGL Technology.

   The supply of both Part 1 and Part 2 DSGL Technology is regulated under the DTCA. Defence Export Controls (**DEC**), which administers the defence export regime, has provided guidance that there won't be a supply for the purposes of the DTCA if information is shared within a company (e.g. if an employee located in Australia provides DSGL Technology to another employee of the same company located overseas). This exception doesn't extend to sharing DSGL Technology between subsidiaries, or for a supply to a contractor.
2. Publication. The second activity regulated under the DTCA is publication of DSGL Technology. This is where a person makes DSGL Technology available to the public or a section of the public. This control only applies to Part 1 Technology.

   Sometimes it can be difficult to draw a distinction between 'supply' (which applies to both Part 1 and Part 2 DSGL Technology) and 'publication' (which only applies to Part 1 Technology). DEC has indicated that there will only be a publication if the technology is made available to the public (even if an individual needs to pay to access the content). However, if there are any restrictions on the particular individuals or groups that can access the DSGL Technology, DEC will treat the transfer as a supply (meaning that such a supply of Part 2 DSGL Technology may be controlled). This conduct commonly occurs within the academic sphere.
3. Brokering. The final type of controlled activity controlled under the DTCA is known as brokering. This occurs where a person acts as an intermediary between two people located outside of Australia in arranging for the supply of goods or technology listed on the DSGL, and applies to all goods and technology listed in Part 1 of the DSGL and to Part 2 goods and technology in certain circumstances[1]. Brokering is less common with R&D activities, but it is subject to strict controls.

1 Part 2 goods will fall within the scope of 'brokering' if the broker knows, or would be reckless or negligent not to know, that the goods or technology are being brokered for a military end-use or a weapons of mass destruction program.

Are there any exceptions?

Unless an exception applies, if the goods or technology and the activity are all controlled, an export permit will be required to transfer the goods or technology outside of Australia.

Some commonly relied-upon exceptions are:

- **Public domain**. Export controls don't apply to technology that is in the public domain (i.e. technology that everyone already has the opportunity to access).
- **Basic scientific research**. This exception applies to technology that is considered 'basic scientific research', defined as 'experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective'. The condition that the research is not 'primarily directed towards a specific practical aim or objective' means many activities performed for a commercial application are unlikely to fall within the exception.
- **Pre-publication**. Supply of DSGL Technology preparatory to publication may be exempt from the DTCA. This exemption is fairly narrow, and applies where an author of an article sends a draft publication overseas to further that publication (e.g. for peer review).
- **Patent exception**. This exception applies to the supply of technology that is the minimum necessary information for a patent application. This exception is also fairly narrow and only applies if the supply is for a purpose directly related to seeking a patent.
- **Oral supply**. An oral supply of DSGL technology is exempt from export controls. For example, communicating information about DSGL Technology on a telephone call or video conference is exempt. However, the supply of other material (e.g. speaking notes or slides) may still be covered.

What should you do if you think your technology might be covered?

If the goods or technology fall within the scope of the DTCA, and your transfer is controlled, an export permit will likely be required to transfer the goods or technology overseas.

In many cases, it can be difficult to determine whether controls will apply. In such cases, DEC encourages potential exporters to submit a DSGL Activity Assessment. DEC will review the information supplied in a DSGL Activity Assessment application and provide an in-principle assessment of the controlled status, allowing exporters to determine the appropriate next steps

If goods or technology are controlled (and no exception applies), an export permit will be required. When applying for a permit, DEC requires information about the goods and technology, their export / supply, and potentially end-users. DEC will review this information to determine the risk posed by the export and therefore whether a permit should be granted. The Action Plan indicates the technology which may significantly impact Australia's national interest, and is likely to be a relevant consideration for DEC when deciding whether to issue an export permit.

If an export permit is granted, exports within the scope of the permit will be permitted. However, an exporter must also comply with obligations, including the maintenance of records about the export or supply for five years.

Penalties for non-compliance

The penalties for breaches of the defence export regime are strict, and may involve personal liability. Under the *Customs Act 1901* (Cth) and the DTCA, exporting or supplying DSGL goods or technology without a permit can result in imprisonment of up to ten years, a fine not exceeding 2,500 penalty units (currently A$525,000 for individuals), or both.

Because of these strict penalties for non-compliance and the risk that technology may be inadvertently controlled, companies or individuals that may transfers goods or technology overseas should have the defence export regime as a priority focus.

Tips for compliance

Due to the technical nature of the DSGL and the broad range of activities controlled, navigating compliance with Australia's defence export regime can be complex.

The following four questions can help guide exporters to determine how to approach defence export compliance:

1. Is the good or technology to be transferred within the scope of the DSGL? The goods, technology and their components should be checked against the parameters specified in the DSGL.
2. Is the transfer to a person located overseas? It's important to consider the identity of the recipient, and the nature of the transfer (e.g. physical exports or supply of intangible technology).
3. Does an exception apply? Some of these exceptions are fairly narrow, and should be carefully considered before being relied on.
4. Is any export permit necessary? If so, what should its scope be – who requires access to the DSGL Technology, and for what purposes?

Changes to Australia's privacy laws: what happens next?

By Philip Catania, Partner, Helen Clarke, Partner, Lynton Brooks, Senior Associate and Viva Swords, Senior Associate

The Australian Government has recently announced two significant proposed privacy reforms.

The first is the introduction of an exposure draft for a new Online Privacy Bill[1] (**Bill**) – which would enable the creation of new binding online privacy codes for social media and other online platforms, as well as significantly increasing penalties and enforcement measures for all organisations found in breach of the *Privacy Act 1988* (Cth) (**Privacy Act**).

The second is the release of an extensive Discussion Paper by the Attorney-General's Department as part of its ongoing review into the Privacy Act, which follows a high level Issues Paper published in October 2020.

The Discussion Paper proposes a number of significant reforms to the Privacy Act, many of which are based on overseas regulations such as the European General Data Protection Regulation (**GDPR**) and the California Consumer Privacy Act (**CCPA**). While amending legislation is yet to be released, if the proposed changes are passed it will represent a significant reshaping of privacy laws in Australia.

Exposure draft of the Online Privacy Bill

Despite the Bill's name, and its primary focus on online platforms, it has significant ramifications for any organisation bound by the *Privacy Act 1988* (Cth) (**Privacy Act**). As foreshadowed by the Australian Government in March 2019, the Bill amends the maximum penalty for corporations that engage in a serious or repeated interference with privacy to the greater of:

- A$10 million;
- three times the benefit of the misconduct; or
- 10% of the organisation's turnover in the 12 month period up to the conduct.

The Bill also introduces:

- new information-gathering powers for the Office of the Australian Information Commissioner (**OAIC**) and an infringement notice mechanism for non-compliance); and
- new declarations that the OAIC can give when making a privacy determination – including the right to require the respondent to prepare and publish a statement about its conduct, and the right to require the respondent to be audited by a qualified independent advisor.

The Bill also provides the framework to deliver on the government's promise to introduce specific privacy rules for online platforms. While the Privacy Act already has a mechanism for sector-specific privacy codes to be developed, a new raft of provisions allow for the Commissioner (or an industry group) to develop an 'online privacy (**OP**) code' for 'OP organisations'. These cover a raft of different matters and additional obligations, which go beyond what a general privacy code could have covered (under existing provisions), including:

- specific privacy policy and collection notice requirements;
- granular requirements in relation to obtaining consent from individuals;
- giving individuals the right to object to the further use or disclosure of their personal information; and
- mandating age verification, to ensure that those giving consent are either 16 years or older, or are the person's parent or guardian.

Organisations subject to an OP code will be:

- social media services;
- data brokerage services;
- large online platforms (which have at least 2.5 million end users in Australia); and
- any other organisations prescribed by law.

1 Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

Discussion Paper for further privacy law reforms

While the Issues Paper released in October 2020 posed a number of questions about the future directions of privacy laws, the Discussion Paper refines those themes into a series of proposed amendments – a number of which will require substantive changes in organisations' personal information handling practices, and their assessment of compliance risks. Many of the changes proposed are based on requirements or concepts found in comparable overseas regulations, such as the European GDPR and the Californian CCPA.

Some of the key highlights include:

1. Definition of personal information. The definition of personal information determines the scope of an organisations' privacy obligations in Australia. The Discussion Paper proposes to broaden both the concepts of 'personal information' and 'collection', so that the laws apply to all information that relates to a person, and to cover personal information that is inferred or generated by an organisation. Therefore, not just information 'about' a person.
2. Privacy policies. The Discussion Paper proposes a number of new matters that must be covered in organisations' privacy policy, including express obligations to:
   - address the use of personal information to influence an individuals' behaviour and decisions and / or in automated decision-making;
   - identify third parties involved in the provision of online marketing materials; and
   - specifically identify the types of personal information that may be disclosed to recipients outside Australia.

   This will mean substantial changes to existing privacy policies.
3. Collection notices. In Australia, there is inconsistent compliance with the requirement to provide personal information collection notices to individuals. The Discussion Paper includes a raft of recommendations aimed at increasing the prominence and usefulness of such notices, including that:
   - notices must be clear, current and understandable;
   - notices must expressly address any indirect collection of personal information (not from the individual), including the entity from whom it was collected;
   - significantly narrowing the circumstances where an organisation cannot give a collection notice (meaning we can expect a proliferation of these notices in the future); and
   - notices must expressly identify the primary purpose of collection, including where that purpose is to influence an individuals' behaviour and decisions.

   These changes represent a desire to provide greater transparency, and may foreshadow increased regulatory attention on organisations' compliance with collection notice obligations.
4. Consent. The Discussion Paper recommends incorporating in the Privacy Act the OAIC's definition of consent. This means consent must be voluntary, informed, current, specific and an unambiguous indication through clear actions. Interestingly, there is no recommendation for consent to be 'freely given' (as was recommended in the Digital Platforms Inquiry report), apparently on the basis that the Attorney-General's Department considers that to be 'equivalent' to the requirement for consent to be voluntary.

   The Discussion Paper also proposes to incorporate the OAIC's guidance that individuals can generally give consent on their own behalf from when they are 16 years old, and otherwise consent is required to be given by a child's parent or guardian.
5. Collection, use and disclosure. The Discussion Paper proposes a number of changes which will narrow the bases on which organisations are permitted to collect, use and disclose personal information. These include:
   - introducing a new overarching 'fair and reasonable' requirement for any collection, use and disclosure of personal information (with factors to be set out in the legislation);
   - defining the 'primary purpose' for collection as the purpose which is notified to the individual;
   - requiring a privacy impact assessment to be undertaken in relation to prescribed practices, such as large scale processing of personal information;
   - for certain sectors, requiring organisations to offer pro-privacy settings by default;
   - requiring organisations that collect personal information indirectly through another party to verify that personal information was originally collected by that other party lawfully; and
   - requiring organisations to keep records of the secondary purposes for which they use and disclose personal information (for the purposes of demonstrating APP 6 compliance).
6. Right to object and portability. Interestingly, the Discussion Paper did not propose to introduce a general right of data portability under the Privacy Act. Australia has taken a sectoral approach to data portability through the Consumer Data Right, which currently applies to the banking sector, and will expand to other sectors over time. The paper notes that introducing a right of personal information portability under the Privacy Act may duplicate aspects of the Consumer Data Right, and create unnecessary complexity.

7. Limited rights of erasure. The Privacy Act does not currently provide a right for individuals to request erasure of their personal information, as exists under some overseas laws such as the GDPR and the CCPA. There are, however, some limited erasure rights in Australia under the Consumer Data Right framework and the My Health Record system.

   The Discussion Paper proposes to introduce a limited right of erasure into the Privacy Act, which would enable individuals to request their personal information be erased in the following circumstances:

   - the information must be destroyed or de-identified under APP 11.2;
   - the information is sensitive information as defined in the Privacy Act;
   - the individual has successfully objected to the handling of their personal information through the proposed right to object discussed above;
   - the personal information has been collected, used or disclosed unlawfully;
   - the organisation holding the information is required by Australian law or a court or tribunal order to destroy the information; or
   - the information relates to a child and the request is made by the child, their parent, or an authorised guardian.

   This right would be subject to certain exceptions, such as where the information is required to complete a transaction or to perform a contract with the individual, where deletion would be technically impractical or impossible, or where there is a public interest in retaining the information (among other proposed exceptions).

8. Right to request source of collection. The paper suggests expanding the existing access rights under the Privacy Act to enable individuals to request, and to require organisations to provide, the source of any personal information about the individual that has been collected by the organisation indirectly through a third party – unless this is impossible or would involve disproportionate effort.

9. Information security. The Privacy Act currently requires organisations that hold personal information to take such steps as are reasonable in the circumstances to protect that information from misuse, interference and loss and from unauthorised access, modification or disclosure.

   The Discussion Paper suggests clarifying that 'reasonable steps' includes both technical and organisational measures. It also suggests including a list of factors to be considered when determining what reasonable steps are required, such as:

   - the nature of the organisation;
   - the amount or sensitivity of the personal information held;
   - the possible consequences for an individual in the case of a breach; and
   - the relative complexity involved in implementing a security measure against the net benefits that measure may provide.

   The paper also proposes strengthening the information destruction requirements under the Privacy Act, by requiring organisations to take **all** reasonable steps to destroy or anonymise personal information when it is no longer needed or required (as opposed to taking such steps as are reasonable in the circumstances).

   The OAIC is, in any event, currently undertaking a review of its Guide to Protecting Personal Information.

10. Overseas data flows and standard contractual clauses. The Privacy Act requires organisations that disclose personal information overseas to take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles in relation to the information.

    An exception to this requirement is where the organisation reasonably believes the overseas recipient is subject to a law or binding scheme that, overall, is at least substantially similar to the Australian Privacy Principles, and there are mechanisms that an individual can access to take action to enforce those protections.

    The Discussion Paper suggests introducing a mechanism to prescribe countries and certification schemes that will satisfy this exception. This would provide greater certainty to organisations when disclosing information to prescribed countries, and would operate like the 'adequacy' system under the GDPR.

    In addition, the paper also proposes the introduction of 'standard contractual clauses' for transfers to overseas countries that are not prescribed, similar to the mechanism under the GDPR. These standard clauses would stipulate how an overseas recipient is expected to handle personal information, and would reduce the regulatory burden on organisations to negotiate appropriate data protection clauses when contracting with overseas entities. Like the GDPR standard contractual clauses, they may also give individuals a direct right to enforce compliance with, or claim damages for non-compliance with, those clauses.

11. Enforcement. The Discussion Paper proposes a bevy of new investigative and enforcement powers for the OAIC, in particular:

    - the introduction of two new civil penalty provisions, to complement the existing civil penalty provision for serious or repeated interferences with privacy. The new civil penalty provisions would include:
      - a mid-tier civil penalty provision for any interference with privacy with, a lesser maximum penalty than for a serious and repeated interference with privacy; and

- a series of new low-level and clearly defined breaches of certain Australian Privacy Principles, with an attached infringement notice regime to enable the OAIC to issue infringement notices without initiating court proceedings;

– enhanced investigative powers which would give the OAIC new powers similar to those exercisable by law enforcement – such as the power to search premises for evidential material, make copies of information and documents specified in a warrant, and to seize evidential material to prevent the destruction of evidence;

– the introduction of a new power for the OAIC to undertake public inquiries and reviews into specified matters; and

– enhanced powers to make determinations requiring an organisation to identify, mitigate, and redress actual or reasonably foreseeable loss.

12. Industry funding arrangement for the OAIC. Under the proposed arrangement, all organisations that receive the benefit of the OAIC's services would pay a cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments.

    A narrower group of entities which operate in a high privacy risk environment (such as social media platforms and organisations that trade in personal information) could also contribute a statutory levy to support the OAIC's management of public inquiries and investigation into their acts or practices.

13. Direct right of action and statutory tort. Currently, there is no direct right of action under the Privacy Act which enables individuals to initiate proceedings in court for breaches of the Act. The Discussion Paper proposes to allow individuals or groups of individuals whose privacy has been interfered with to commence proceedings in the Federal Court or Federal Circuit Court.

    Claimants would first need to make a complaint to the OAIC, or the proposed new Federal Privacy Ombudsman, and have their complaint assessed for conciliation, before commencing action in court. Complainants would also need the leave of the court to make an application.

    In addition to this statutory right, the paper also considers the introduction of a new tort for invasions of privacy. Four options are considered:

    – a statutory tort for invasion of privacy with two limbs – intrusion upon seclusion and misuse of private information;

    – a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts;

    – do not introduce a statutory tort, but extend the application of the Privacy Act to individuals in a non-business capacity for collection, use, or disclosure of personal information which would be highly offensive to an objective reasonable person; and

    – legislating that damages for emotional distress are available for equitable breaches of confidence.

14. Controller and processor distinction. Although no specific proposals are put forward, the Discussion Paper raises the question as to whether the Privacy Act should introduce a distinction between 'controllers' (entities who determine the purpose and means of any processing) and 'processors' (entities that process personal information on the instructions of a controller). The controller / processor distinction is recognised in many overseas privacy laws, such as the GDPR.

15. Exemptions. The Discussion Paper also considers whether there is a need to modify or remove the exemptions currently in the Privacy Act for employee records, registered political parties, and journalism, in light of the other proposed changes in the paper. However, no specific proposal has been put forward in the Discussion Paper regarding these exemptions at this stage.

What happens next?

Submissions on the exposure draft of the Online Privacy Bill were due by **3 December 2021**. The Bill will now be updated and introduced to Parliament.

If passed, the enforcement and penalties changes will take effect immediately on the Act receiving Royal Assent. The online privacy code provisions will take effect on a date fixed by proclamation, within 12 months of the Act receiving Royal Assent.

Submissions on the Discussion Paper for the Privacy Act review can be made to the Attorney-General's Department until **10 January 2022**. The Discussion Paper contemplates that there will be a further Final Report following the public consultation process, which will be considered by the Australian government. The government will then consider what reforms, if any, it wishes to make to the Privacy Act following its review of the Final Report.

Technology and human rights: emerging risks for companies and boards

By James North, Head of Technology, Media and Telecommunications, Dr Phoebe Wynn-Pope, Head of Business and Human Rights and Thomas Milner, Law Graduate

As Australia treads a rapid path towards becoming a leading digital economy, corporates are increasingly adopting emerging technologies, including artificial intelligence (**AI**), to assist with various business operations and functions.

But while novel technologies offer exciting commercial opportunities, they can also create new legal, reputational and human rights risks that companies and boards should be taking proactive steps to mitigate.

Directors and managers should understand the technology they are deploying in the business, in order to be able to assess and mitigate any risks arising from its use. These risks can be varied and in some cases extremely complex, requiring subject matter expert consideration of the technology and its impacts from the design stage through to end use.

Liability risks for AI-informed decision-making

Companies may incur liability for unlawful decisions made using AI-informed technology. AI systems make decisions based on analysis of large databases, which may include data relating to historical human-made decisions. If that data indicates a trend of bias (for example, due to historically prevalent prejudices), that bias may be replicated in the decisions made by the AI system.

Similarly, AI systems use algorithms that may reflect the prejudices of the engineers that developed them. If a company makes an AI-informed decision which is discriminatory due to underlying bias in the data set or algorithms – such as a hiring decision which factors in protected attributes such as race or gender – it may be liable for breach of anti-discrimination law.

Liability risks are likely to increase as regulation of AI use expands. For example, the Australian Human Rights Commission has recommended a moratorium on the use of biometric technology due to the high risk of human rights impacts. Companies should ensure that their deployment of AI does not conflict with expanding regulation.

How can liability risks be mitigated?

There are a number of measures and processes that companies and general counsel can put in place to verify appropriate AI-informed decision-making, including:

- **Obtaining contractual protections from the provider of the AI system**. These may include warranties that the AI system is fit for purpose and has been trained on appropriate data, or indemnities against the liability resulting from discrimination in the AI system.
- **Taking operational steps to minimise the risk of harm resulting from its use of AI**. These may include ensuring that the AI system is rigorously tested in a safe environment prior to commercial use, that the data used to train the AI system is fit for purpose and free from biases, that the operation and decisions made by the AI is subject to appropriate human oversight, and that appropriate procedures are put in place to handle complaints and redress any unintended harm.
- **Ensuring that an audit is conducted to determine what AI systems are already in use at the company or are proposed for future use**. This will help general counsel understand the relevant risks that might arise from the company's use of AI systems, and what mitigation measures would be appropriate to address those risks.

Directors' duties and personal liability

As the use of technology expands, it is expected that directors will increasingly seek to use machine learning and AI to assist them in their own decision-making. At a minimum, directors will likely rely on AI-informed decisions taken elsewhere within the organisation. Where the AI is wrong, or has been built on flawed data-sets, wrong decisions or even decisions that breach the law may result.

The question for directors is whether they may be exposed to a breach of their statutory duty to exercise reasonable care and diligence. For example, directors are obligated to inform themselves about the subject matter of business decisions to the extent that they reasonably believe to be appropriate. It may be difficult for directors to comply with this obligation if they rely upon the conclusions drawn by an AI system when they do not fully understand the operation of that system.

How can directors' risks be mitigated?

Steps that directors can take to mitigate their risks of breach of statutory duties and personal liability for AI-informed decision-making include:

- **Ensuring that an audit is conducted to determine what AI systems are already in use at the company or are proposed for future use**. An AI audit helps directors understand what information and decisions they are making has been influenced or informed by AI, and empower them to further interrogate aspects and operation of the AI where necessary.
- **Requiring management to implement human rights safeguards**. These may include conducting human rights impact assessments for each system and ensuring human oversight over the operation of the system to minimise the risks of unexpected bias in decisions.
- **Increasing the technology capabilities of the board through targeted training**. This will enable the board to provide appropriate oversight of the company's use of AI. A recent study by the Australian Institute of Company Directors and the University of Sydney showed that only 3% of surveyed company directors brought technological expertise to the board.

Reputational and human rights risks of AI use

Even if companies do not incur liability for technology-assisted decisions, they may still suffer reputational damage and associated loss of public trust if those decisions impact upon human rights. Even if a company's AI systems do not make harmful decisions, non-transparent AI-informed decisions may contribute to public distrust of the company.

The risk of reputational damage associated with AI is particularly high in a social context of low public trust in AI – a recent report by the University of Queensland and KPMG indicated that only one in three Australians currently trust AI technology.

How can human rights and reputational risks be mitigated?

There are several voluntary tools that companies may use to reduce their reputational and liability risk and ensure that their AI systems are safe, secure and reliable. For example, the Australian Government has introduced voluntary AI Ethics Principles, which encourage companies deploying AI to ensure that:

- they respect human rights;
- they protect diversity and the autonomy of individuals;
- the outcomes of their decisions are fair and remain inclusive and accessible;
- there is a measure of transparency and explainability on any decisions made using AI;
- consumers are able to contest those decisions; and, ultimately
- those responsible for the deployment of the technology are accountable for the decisions that result.

Further, the Australian Human Rights Commission has recommended private sector adoption of human rights impact assessments to determine how their use of AI systems engages human rights, and the compliance measures that can be taken to ensure that human rights are not violated.

Looking ahead

As we look ahead to a future in which emerging technologies will play an increasingly important role, it is vitally important that companies and boards take proactive steps to mitigate the associated legal, reputational and human rights risks.

eSafety in Australia: an overview of the strengthened *Online Safety Act 2021*

By Philip Catania, Partner, Robert Ceglia, Associate and Allison Inskip, Paralegal

Over recent years, cyber-bulling has become increasingly common, with an estimated one in five children being socially excluded, threatened or abused online. The Australian Parliament has actively sought to address this issue, and in 2015, it introduced legislation to establish the world's first 'eSafety Commissioner'. The eSafety Commissioner's role was to promote online safety and investigate complaints about the existence and sharing of cyber-bulling material.

In June 2021, the Australian Parliament passed new legislation to significantly expand the eSafety Commissioner's powers – the *Online Safety Act 2021* (Cth) (**OSA**). When the law comes into effect (on 23 January 2022), the eSafety Commissioner will have broad powers to order a range of individuals, websites and other online service providers to remove content and block sites that host or share prohibited material.

This article summarises some of the eSafety Commissioner's new powers and the impact they may have on individuals and businesses providing services online.

Evolution of the *Online Safety Act 2021* (Cth)

In 2015, the Australian Parliament passed the *Enhancing Online Safety Act 2015* (Cth) (**EOSA**) which created the world's first 'eSafety Commissioner' (originally known as the 'Children's eSafety Commissioner). Under the EOSA, the eSafety Commissioner was responsible for promoting online safety for children, conducting research into online safety for children and investigating complaints about cyber-bulling material that targeted an Australian child. To support these functions, the eSafety Commissioner was also granted powers under other laws (including the *Broadcasting Services Act 1992* (Cth)).

In 2017, the EOSA was amended so that the eSafety Commissioner could exercise its rights to protect all Australians from cyber-abuse and cyber-bullying (not just children).

While the eSafety Commissioner was fundamental in driving change and raising awareness of online safety in Australia, an independent report issued by Lynelle Briggs AO in 2018 into the effectiveness of the EOSA recommended major reforms to Australia's eSafety regime. The report concluded that major reforms were necessary because the existing legislative framework was fragmented, out-of-date and constrained the eSafety Commissioner's ability to operate effectively (particularly due to the broad governance arrangements).

The report ultimately recommended that the EOSA and eSafety Commissioner's powers under other laws consolidated into a new 'Online Safety Act' and code of industry practice.

In December 2019, the Commonwealth Government commenced public consultation for the new Online Safety Act, and on 23 December 2020 it released an exposure draft of the Online Safety Bill 2020 (Cth).

After several changes were agreed in the Senate, the OSA passed through both houses of parliament and will come into effect on 23 January 2022.

Who does the *Online Safety Act 2021* (Cth) affect?

Once the OSA comes into effect, it will impose obligations on a very broad range of businesses – essentially any business that provides internet services or that allows individuals to communicate online.

In particular, the OSA will impact entities that provide any of the following services:

- **Social media services** – this category is defined broadly to include any electronic service whose sole or primary purpose is to enable online interaction between users (e.g. Twitter and YouTube).
- **Relevant electronic services** – this category covers electronic services that enable end-users to communicate by email, instant messaging, SMS, MMS, chat or to play online games with other end-users (e.g. Gmail, Discord, the chat feature of video games).
- **Designated internet services** – this category includes services that provide end-users with access to material using an internet carriage service (e.g. Safari and Mozilla).
- **Hosting service providers** – this category covers entities that host material that was provided on any of the above services (e.g. AWS and Azure).
- **Internet service providers** – this category means any person that supplies or proposes to supply an internet carriage service to the public (e.g. nbn, Telstra and Optus).
- **App distribution service providers** – this category relates to services that allows end-users to download apps (e.g. Google Play, the Apple App Store and Steam).

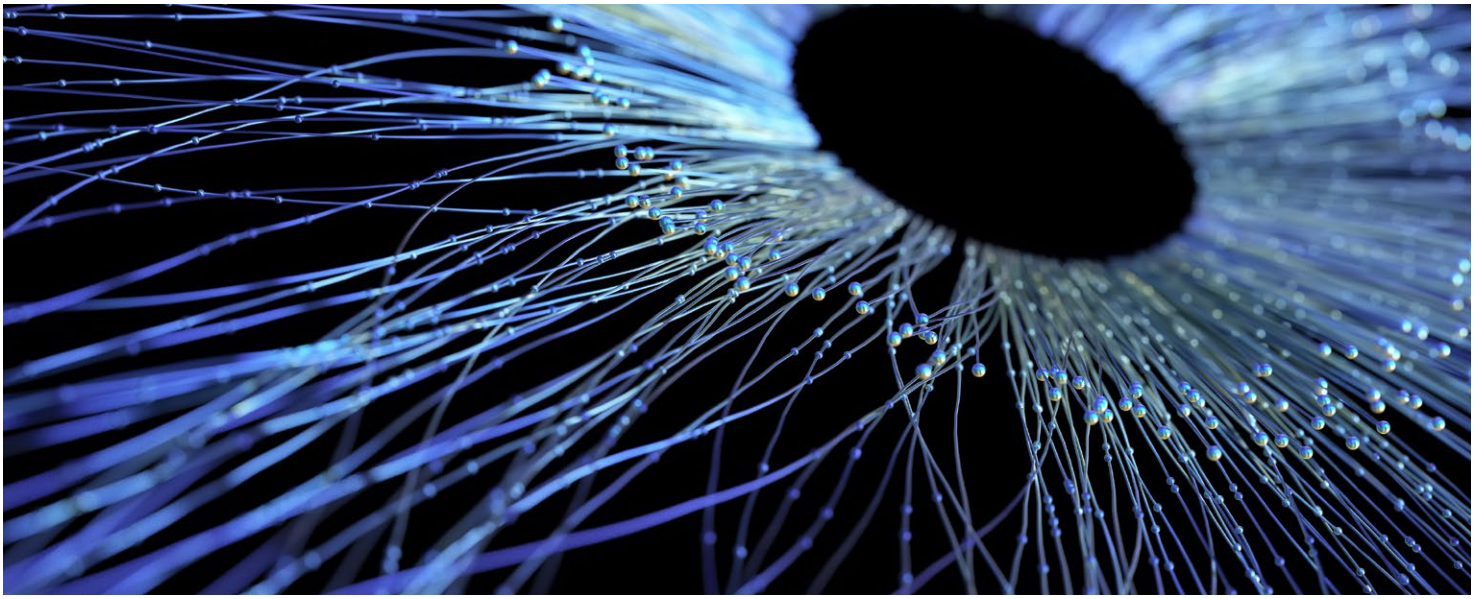
The OSA will also extend to acts, omissions, matters and things outside Australia, which is designed to ensure the protections under the OSA apply even if content is hosted overseas (see section 23(2)). This applies whether it is Australian children or adults being targeted or end users in Australia can access the relevant material.

How does the *Online Safety Act 2021* (Cth) aim to enhance online safety?

The OSA aims to improve online safety for Australians by preventing the following types of content being shared online and which end users in Australia can access:

- **Cyber-bullying material** – this category concerns material that likely targets a particular **Australian child**, and would likely be seriously threatening, seriously intimidating, seriously harassing or seriously humiliating.
- **Cyber-abuse material** – this category concerns material intended to cause serious harm to a particular **Australian adult** and an ordinary reasonable person would regard the material as being menacing, harassing or offensive.
- **Intimate images** – this category concerns material that depicts a person's private parts, private activity or a person without attire of religious or cultural significance.
- **Class 1 and Class 2 material** – Class 1 material is material that has been Refused Classification under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). Class 2 material is material that has been classified as X18+ or R18+ under that scheme.
- **Abhorrent violent conduct** – this category involves material that depicts a terrorist act, murder or attempted murder, torture, rape or kidnapping.

In order to prevent such material being shared online, the OSA imposes the following 'proactive' and 'reactive' obligations on a broad range of online service providers.



Proactive obligations – Compliance with the Basic Online Safety Expectations

The OSA introduces a mechanism that allows the eSafety Commission to introduce standards known as the Basic Online Safety Expectations (**BOSE**). An exposure draft of the BOSE is available here.

At a high level, the BOSE will require certain online service providers to take reasonable steps to:

- ensure that end-users are able to use the service in a safe manner;
- minimise the availability of cyber-bullying, cyber-abuse and abhorrent violent material and non-consensual intimate images;
- have clear and readily identifiable mechanisms to allow end-users to make complaints and report breaches of a provider's Terms of Use; and
- implement technical controls to limit children's access to certain material.

Currently the BOSE only applies to businesses that provide a 'social media service', a 'relevant electronic service' or a 'designated internet service' (see above).

Compliance with the BOSE is supported by the OSA in the following ways:

- First, the eSafety Commissioner can require businesses to report on their compliance with the BOSE. Civil penalties of up to A$550,000 apply if the business does not respond.
- Second, the eSafety Commissioner can identify providers that do not meet the BOSE on its website – this could have a significant reputational impact for an online service provider.
- Third, the eSafety Commissioner can publish statements of compliance on its website for online service providers that comply with the BOSE – again, this could be a reputational differentiator for businesses seeking to provide safe online service.

A final version of the BOSE is expected to be issued in early 2022.

Reactive requirements – compliance with takedown and blocking notices

In addition to the introduction of the BOSE, the OSA provides the eSafety Commissioner with the power to issue online service providers with takedown and blocking notices. The specific type of notice will vary slightly depending on the nature of the online service provider's business.

In summary, the eSafety Commissioner's notices can:

- compel online service providers to remove cyber-bullying, cyber-abuse and non-consensual intimate image materials within 24 hours of receiving the notice (previously businesses had 48 hours to remove such content);
- compel online service providers to remove material that has (or would have) a Refused Classification within 24 hours (ie Class 1 material). The eSafety Commissioner can also issue a notice to search engine providers and app distributors to remove links of apps that may have Refused Classification content;
- compel online service providers to remove (within 24 hours) material that has (or would have) the restrictive classifications of X 18+ or R 18+ where it is accessible to end-users in Australia (i.e. Class 2 material);
- require online service providers to provide information about the identity of an end-user of a service (including their contact details) where the information is relevant to the operation of the OSA; and
- issue a 'blocking notice' to compel an internet service provider to disable access to abhorrent violent material. This notice power is in addition to powers that already exist under the Commonwealth Criminal Code.

Civil penalties of up to A$550,000 apply for failure to comply with a notice issued by the eSafety Commissioner.

Key takeaways

The OSA will come into effect on 23 January 2022 and will have a significant impact on businesses that provide internet services or allows individuals to communicate online. Currently the only 'unknown' is the full scope of the BOSE – the Government has only issued an exposure draft of the BOSE on which it sought feedback until 12 November 2021.

Following this feedback, the Minister for Communications, Urban Infrastructure, Cities and the Arts will consider submissions and make a final Online Safety (Basic Online Safety Expectations) Determination, which is expected to come into effect at the same time as the OSA.

For businesses who are likely caught by the OSA, there are some steps they can take to help prepare for the introduction of the OSA:

1. Review the exposure draft of the BOSE (available here). This will provide businesses with an idea about the types of requirements the eSafety Commissioner is likely to introduce.
2. Look at their existing systems and processes to determine whether they are capable of meeting the changes under the OSA (including responding to takedown and blocking notices within a shortened period).
3. Engage in a staff educational process to highlight the key aspects of the OSA.
4. Make or introduce internal governance and policy changes to give effect to the requirements of the OSA.

Australia as a Technology and Financial Centre: unpacking the final report into the digital asset sector

By Steven Rice, Partner, Mizu Ardra, Special Counsel and Chenjie Ma, Associate

The final report on Australia as a Technology and Financial Centre outlines a comprehensive and ambitious plan for Australia to lead the digital assets and blockchain era.

In October 2021, the Senate Select Committee on Australia as a Technology and Financial Centre (**Committee**) released its final report (**Report**).

Background

The Report represents the final phase of the Committee's inquiry into key areas affecting the competitiveness of Australia's technology, finance and digital asset industries. The Committee has previously published interim reports on financial and regulatory technology, including the impact of COVID-19 on technological change, tax incentives, the Consumer Data Right, and skills and talent.

The key purpose of the Report was to focus on financial technology, such as the regulation of cryptocurrencies and digital assets, and the access of fintechs to financial services.

The Government is yet to provide its formal position on the Report. If the Government were to adopt one or more of the Report's recommendations, it could have a significant impact on the Australian fintech landscape and the financial institutions, fintechs and other businesses looking to benefit from digital assets, decentralised blockchain and other distributed ledger technologies.

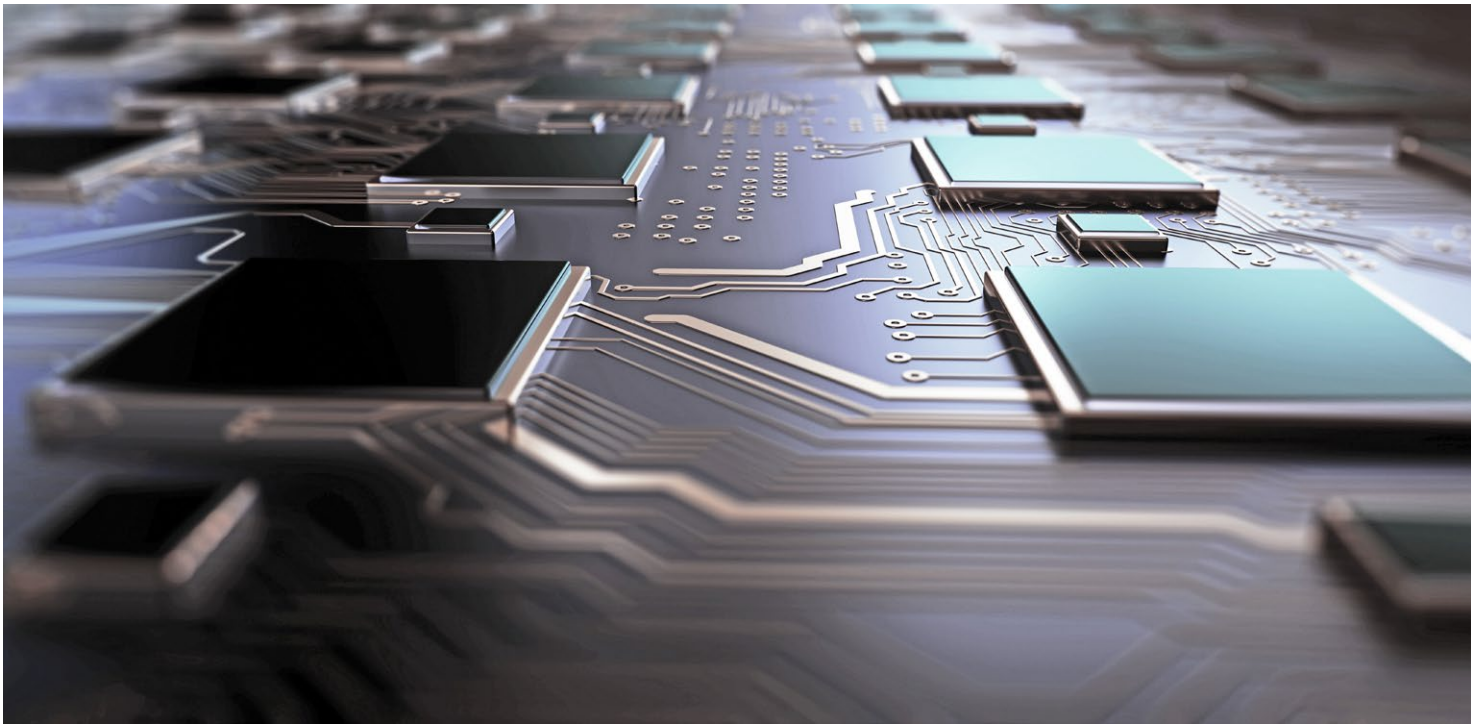
Some of the recommendations build on the findings of other recent inquiries into payments system including the Payments System Review.

The Australian Government may choose to consider these recommendations as part of the broader design of its financial system policies.

Key takeaways

The Report makes 12 recommendations.

1. The Report recommends the Government establishes a new market licence regime for Digital Currency Exchanges (**DCE**). This will supplement the current AUSTRAC 'light touch' registration process. It would be separate to the current Australian market licence regime in the *Corporations Act 2001* (Cth) (**Corporations Act**).
2. The new DCE market licence regime would include, at a minimum, requirements on capital adequacy, auditing and responsible person tests to ensure operational integrity and consumer protection.
3. It is recommended in the Report that the Government implements a custody or depository regime for digital assets with minimum standards. The Report notes that there are unique vulnerabilities relating to custody of digital assets and currently there are limited consumer protections in place for custody services provided for consumers holding crypto-assets.
4. A new legal structure, the 'Decentralised Autonomous Organisation' (**DAO**), is recommended in the Report to be introduced in the Corporations Act. A DAO structure operates on decentralised blockchain infrastructure, with operations pre-determined in open source code and enforced through smart contracts. If this recommendation was adopted, it would give DAO separate legal entity status, and will enable large scale DAO projects to be established in Australia with greater legal certainty for the members.
5. The proposed DAO structure recognises the rapid uptake of decentralised finance applications and other blockchain projects that are typically set up with a decentralised ownership structure. 'Decentralised finance' is an umbrella term for a financial system which functions without intermediaries and is operated by smart contracts and challenges the traditional forms of finance.



6. To keep the options open for future development in digital currency, the Report recommends that the Treasury leads a policy review of the viability of a retail Central Bank Digital Currency (**CBDC**) in Australia. Such a review would build on existing work the RBA is undertaking which explores options for a wholesale CBDC. To date, the RBA has not seen a public policy case for implementing a retail CBDC in Australia.
7. The Report recognises that 'de-banking' of fintechs is a complex problem occurring for a number of reasons, including regulatory arrangements and penalties for non-compliance with anti-money laundering and counter-terrorism financing (**AML / CTF**) laws.
8. The Report recommends that AML / CTF laws be clarified to ensure they are fit for purpose, do not undermine innovation, and give consideration to the driver of the Financial Action Task Force's 'travel rule' (a rule that requires virtual asset service providers to obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers).
9. The Report agrees with the final report on the *Payments System Review* that the Reserve Bank of Australia should develop a set of common access requirements for the New Payments Platform.
10. It is recommended in the Report that a clear process for businesses that have been de-banked should be established including through access to Australian Financial Complaints Authority jurisdiction.
11. The Committee recommends in the Report that the capital gains tax (**CGT**) regime is made clearer so that digital asset transactions only create CGT events where they genuinely result in a clearly definable capital gain or loss.
12. To incentivise sustainable crypto-mining activity in Australia, the Report recommends that businesses undertaking digital asset 'mining' and related activities in Australia should receive a 10% company tax discount where renewable energy is used in these activities.

ASIC's new guidance on crypto-asset exchange traded products and other investment products

Since the publication of the Committee's final report, ASIC has independently published Information Sheet 225 *Crypto-assets* and Information Sheet 230 *Exchange traded products: Admission guidelines* (**Info Sheets**). The Info Sheets set out what ASIC considers to be good practices principles relating to product issuers and market operators on meeting their regulatory obligations in relation to crypto-asset exchange traded products and other investment products.

What happens next?

The Australian Government may choose to provide its formal position on the recommendations made in the Report. It may do so as part of a broader response to other recent inquiries into the regulation of the Australian payments system.

For now, the industry must watch and wait for the outcome.

Australia's digital identity framework: opportunities for banks, telecommunications and other service providers

By Helen Clarke, Partner and Viva Swords, Senior Associate

Australia has released an exposure draft of legislation to regulate its Trusted Digital Identity Framework (**TDIF**), so the framework can be rolled out economy-wide. While some digital identity services are already commercially available, there may be a greater uptake of TDIF-accredited solutions, as they will be subject to added privacy and security safeguards, and will be interoperable with other organisations in the digital identity ecosystem.

Government and private sector service providers should start considering how they will take advantage of developments in Australia's digital identity framework.

Reducing the hassle of identity checks

Digital identities promise an end to individuals having to provide copies of identification documents to each separate service provider that needs to verify their identity.

The TDIF offers a model where an identity service provider (such as Australia Post's 'Digital iD' or the ATO's 'myGovID') verifies an individual's identity documents once. If an individual then needs to verify their identity to a 'relying party' (a service provider to the individual), the individual can request the identity service provider to confirm to the relying party that it has performed that verification. The identity service provider only gives the relying party minimal amounts of personal information – such as name, contact details, and date of birth.

Essentially, the identity service provider says: 'I have verified Jane Smith, born 1 January 2001 [to a particular assurance level]. You can rely on that verification and don't have to undertake it yourself.'

This system is clearly underpinned by trust – trust in the verification undertaken by the identity service provider – because the relying party won't receive its own copy of the individual's detailed identification information. The TDIF aims to generate this trust.

How does the TDIF work?

The TDIF, which has been iteratively developed by the Digital Transformation Agency (**DTA**) since 2015, provides for an accreditation system with the following roles:

- **identity service providers** that help individuals (users) set up and manage a digital identity account (currently, accredited providers are the ATO's myGovID and Australia Post's Digital iD);
- **credential service providers** that manage credentials used in the system (e.g. passwords);
- **identity exchanges** that provide the infrastructure for the system and manage the transfer of information (currently the Department of Human Services); and
- **attribute service providers** that provide specific authoritative information about a user, such as their qualifications (currently the ATO's Relationship Authorisation Manager which confirms whether a person is entitled to act on behalf of an organisation for taxation purposes).

The system is intended to facilitate a relying party being given the minimal amount of personal information needed for a transaction – for example, instead of an individual proving they are over 18 by showing a proposed service provider evidence of their date of birth, the system can confirm that the person is over 18.

In addition to detailed technical and functional requirements, the TDIF contains rigorous requirements in relation to security and privacy of information, updated to the latest Commonwealth Government requirements. It also provides for different levels of assurance, so that a service provider can specify a required level of identity verification commensurate to the transaction (e.g. paying a parking fine, compared with undertaking a significant financial transaction).

The TDIF is currently a standalone policy framework. However, the Australian Government has recently released draft principal legislation under which the TDIF and participants will operate.

Currently, the TDIF is used to provide access to a range of federal government services, such as myGov and establishing a Unique Student Identifier. The DTA is looking to make digital identity solutions available to services across the economy, through the accreditation and assurance processes in the TDIF.

What does this mean for service providers?

Some private sector service providers may be interested in developing systems and becoming accredited as an identity service provider, credential service provider, an identity exchange or an attribute service provider (if they handle attributes about an individual that other organisations may want to verify).

The draft legislation contemplates that entities fulfilling these roles will receive payment through charges levied on relying parties, however the proposed charging mechanism is yet to be developed in detail.

Other service providers such as banks, telecommunications providers and utilities, as well as Federal, State and local government agencies, may be looking to adopt digital identity solutions to streamline identity verification of their customers.

While some digital identity solutions are already commercially available, the DTA appears to anticipate that consumers will prefer TDIF-accredited options, which will be subject to legislative privacy and security safeguards, and oversight by an independent authority. It is proposed that TDIF participants will be able to use a 'trust mark' (yet to be developed) to easily identify TDIF-accredited providers.

TDIF-accredited solutions also have the benefit of:

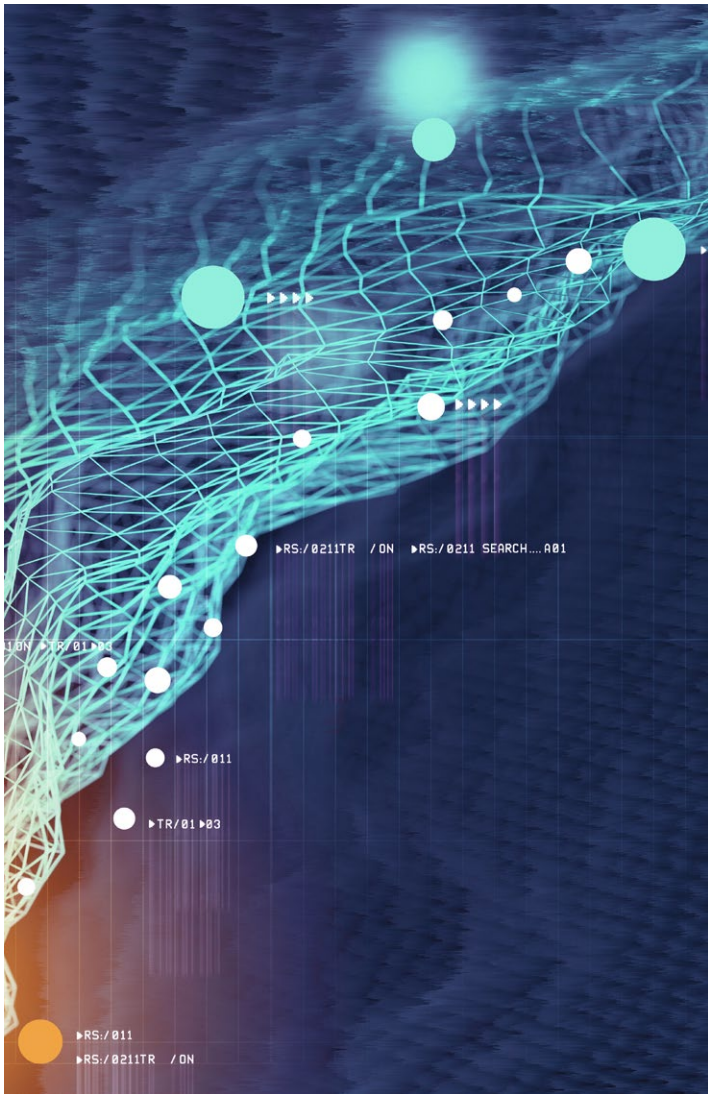
- being interoperable with other entities in the ecosystem, for example, being able to take advantage of new attributes when a new attribute service provider is on-boarded; and
- knowing that the scheme ensures compliance with relevant laws, such as the *Privacy Act 1988* (Cth) (**Privacy Act**), without each participant having to conduct due diligence in relation to the other participants.

However, it is worth noting that, in general, digital identity solutions will not subsume all identity verification processes. Establishing a digital identity will be voluntary for individuals. As such, most businesses will need to retain some alternative processes for individuals who have not elected to go digital.

Reducing online anonymity

The use case for digital identity is expanding. While to date people have been able to use social media and digital platforms anonymously, Federal and state governments are now considering mandating identity requirements to reduce technology-based abuse and bullying.

At the same time, regulators – including competition and data privacy regulators – are increasingly focused on social media and other digital platforms and their collection and handling of personal data. The recently released Online Privacy Bill proposes the development of an 'Online Platforms Code' which will include obligations beyond the existing Australian privacy obligations – including mandatory age verification to determine whether a person can give consent on their own behalf.



Exposure draft legislation to underpin Australia's digital identity ecosystem

Rounds of consultation into proposed digital identity legislation to underpin the TDIF commenced in late 2020, and have culminated in the recent publication of an exposure draft of the Trusted Digital Identity Bill.

The key features of the proposed digital identity scheme proposed in the draft Bill are as follows:

1. A permanent, independent 'Oversight Authority' will be established as an independent statutory officeholder within the Department of Treasury, the Department of Prime Minister and Cabinet, or the ACCC. That officeholder will be supported by the Office of the Oversight Authority, an Advisory Board and a series of Advisory Committees. Advice could be provided on matters of privacy, security and user experience.
2. The Office of the Australian Information Commissioner (**OAIC**), Australia's privacy regulator, will be responsible for the additional privacy safeguards under the scheme (similar to its role under the Consumer Data Right (**CDR**) scheme).
3. The digital identity legislative framework will comprise:
   - the Trusted Digital Identity Bill;
   - general and TDIF rules, which are disallowable instruments;
   - technical standards, which are published by the Oversight Authority; and
   - administrative guidelines, which may prescribe administrative steps for accreditation and other processes.
4. There are a number of privacy safeguards proposed in the Bill, which enshrine a number of existing privacy requirements under the TDIF. In addition to the requirements of the Privacy Act, these include:
   - restrictions on data profiling;
   - restrictions on the collection and use of biometric information;
   - requirements for users' express consent (which we envisage will be similar to some CDR requirements);
   - prohibitions on disclosure for law enforcement purposes;
   - prohibitions on using digital identity information for marketing purposes;
   - restrictions on disclosing a user's identifier;
   - limits on retaining user attributes at the end of a session; and
   - requirements to conduct Privacy Impact Assessments, if required by the Oversight Authority.

   The inclusion of a separate set of privacy safeguards will disappoint some stakeholders, who raised issues with the existing number of separate conflicting privacy schemes under different pieces of legislation,[1] and the compliance burden associated with having a separate scheme in relation to digital identity.

   The draft legislation proposes that 'state or territory' government bodies who participate in the system and who are subject to 'comparable' 'state or territory' privacy laws will not be required to comply with the Privacy Act. However, if 'state or territory' laws do not include a notifiable data breach scheme, 'state or territory' participants will be required to comply with specific notifiable data breach obligations in relation to digital identity data breaches.
5. There will be a number of consumer safeguards included in the Trusted Digital Identity Bill and Trusted Digital Identity Rules, including:
   - a prohibition on creating and using a single identifier across the system;
   - the requirement that entities offer an alternate identity verification method to digital identity, with some exceptions;[2]
   - strict limitations on certain restricted attributes, which can only be handled by specific entities subject to authorisation by the Oversight Authority; and
   - the requirement for identity exchanges to provide consumers a dashboard showing what information has been shared with relying parties.
6. The draft legislation proposes a two stage approach to participation in the digital identity system. The first stage, 'TDIF accreditation', is granted when the entity is verified as meeting the TDIF requirements (this stage does not apply to relying parties). The second stage is for on-boarding entities that actually want to operate within the TDIF, including relying parties. The second stage test includes considerations of national security, meeting rules, risks to the system, and whether they are a fit and proper person.
7. This staged approach is intended to allow entities to seek accreditation even if they are not ready to be on-boarded, or do not want to participate in the system. This may allow the entity to use TDIF trustmarks, even if operating outside the system.

1 For example, under the *Privacy Act 1988* (Cth), the *Telecommunications Act 1997* (Cth) and the Consumer Data Right scheme in Part IVD of the *Competition and Consumer Act 2010* (Cth).

2 Proposed exceptions include organisations who are authorised by statute to conduct certain activities digitally (such as the ATO). The Oversight Authority may issue an exemption, including on the basis that the applicant is a small business or an online-only business.

8. The draft legislation sets out proposed obligations on relying parties, which are broad and not unexpected. They include:
   - notifying the Oversight Authority of security or fraud events;
   - keeping details on the public register of relying parties up to date;
   - complying with conditions on using and sharing attributes;
   - meeting extra requirements in relation to restricted attributes (if authorised to handled them); and
   - complying with payment terms and other on-boarding terms.
9. Submissions on consultations prior to the draft legislation indicated that two topics were of particular interest to prospective relying parties: liability and the charging framework.

   The draft legislation and guide to the framework includes some high level principles about the charging framework, but does not indicate what it will ultimately look like. A preliminary view of a charging framework has been developed and will be continually refined based on ongoing consultation with system participants.

   The draft legislation includes some answers in relation to the proposed mechanisms for dealing with liability and redress. In brief, these are that:
   - an organisation will not be liable for losses suffered by a third party if it has acted in good faith and complied with the requirements in relation to accreditation and the system;
   - the legislation will establish a statutory contract between participants, under which participants are liable for loss suffered by other participants where the liable party has failed to comply with the requirements;
   - in relation to losses suffered by individuals, the position paper suggests that participants will be required to take steps to assist individuals, such as re-establishing digital identities after identity theft or a cyber security incident – the Oversight Authority can advocate on behalf of victims of identity theft; and
   - this scheme will be underpinned by requirements to hold adequate insurance.
10. There will be a range of administrative sanctions and civil penalties available for contraventions of requirements. Administrative sanctions can be imposed by the Oversight Authority. Civil penalties (including for breaches of privacy requirements) will be available under standard regulatory powers mechanisms, in addition to other enforcement options such as enforceable undertakings and injunctions.

    Stakeholders and interested parties were invited to provide comments on the exposure draft legislation by 27 October 2021.

    The Australian Government is considering submissions that it has received, and will publish further information about those submissions prior to introducing the Bill to Parliament.

    The Government has indicated that the charging framework will be developed separately from, and after, the Trusted Digital Identity Bill. This appears to be on the optimistic assumption that the charging framework will not limit uptake of the system by relying parties – an assumption that seems contrary to a number of submissions made during earlier rounds of consultation.

    Beyond just 'watching this space', businesses should be engaging with developments in digital identity at an early stage, as there may be opportunities to ready business processes and technical systems for the adoption of digital identity solutions.

Contacts

James North

Partner and Head of Technology, Media and Telecommunications

+61 2 9210 6734
+61 405 223 691
james.north@corrs.com.au

Eugenia Kolivos

Partner

+61 2 9210 6316
+61 407 787 992
eugenia.kolivos@corrs.com.au

Adam Foreman

Partner

+61 2 9210 6827
+61 431 471 355
adam.foreman@corrs.com.au

Frances Wheelahan

Partner

+61 3 9672 3380
+61 419 517 506
frances.wheelahan@corrs.com.au

Arvind Dixit

Partner

+61 3 9672 3032
+61 438 278 463
arvind.dixit@corrs.com.au

Gaynor Tracey

Partner

+61 2 9210 6151
+61 423 859 363
gaynor.tracey@corrs.com.au

David Yates

Partner

+61 8 9460 1806
+61 414 465 928
david.yates@corrs.com.au

Grant Fisher

Partner

+61 3 9672 3465
+61 407 430 940
grant.fisher@corrs.com.au

Eddie Scuderi

Partner

+61 7 3228 9319
+61 419 731 560
eddie.scuderi@corrs.com.au

Helen Clarke

Partner

+61 7 3228 9818
+61 411 399 643
helen.clarke@corrs.com.au

Jonathan Farrer

Partner

+61 3 9672 3383
+61 414 235 063
jonathan.farrer@corrs.com.au

Michael do Rozario

Partner

+61 2 9210 6566
+61 416 263 102
michael.do.rozario@corrs.com.au

Jürgen Bebber

Partner

+61 3 9672 3260
+61 412 082 114
jurgen.bebber@corrs.com.au

Philip Catania

Partner

+61 3 9672 3333
+61 419 320 815
philip.catania@corrs.com.au

Justin Fox

Partner

+61 3 9672 3464
+61 417 220 275
justin.fox@corrs.com.au

Richard Leder

Partner

+61 3 9672 3489
+61 418 170 790
richard.leder@corrs.com.au

Kate Hay

Partner and
Head of Intellectual Property

+61 3 9672 3155
+61 400 628 372
kate.hay@corrs.com.au

Simon Johnson

Partner

+61 2 9210 6606
+61 412 556 462
simon.johnson@corrs.com.au

CORRS
CHAMBERS
WESTGARTH

This publication is introductory in nature. Its content is current at the date of publication. It does not constitute legal advice and should not be relied upon as such. You should always obtain legal advice based on your specific circumstances before taking any action relating to matters covered by this publication. Some information may have been obtained from external sources, and we cannot guarantee the accuracy or currency of any such information.

Sydney
Melbourne
Brisbane
Perth
Port Moresby

corrs.com.au

BRO0055