BCA
Business Council of Australia

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

November 2022

Contents

1. About this submission

This is the Business Council's submission on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill). The Bill amends three Commonwealth Acts to increase penalties for serious or repeated interferences with privacy, enhances the Australian Information Commissioner's (OAIC) enforcement powers, and provides the Commissioner and the Australian Communications and Media Authority (ACMA) with greater information sharing powers.

The Business Council represents businesses across a range of sectors, including manufacturing, infrastructure, information technology, mining, retail, financial services and banking, energy, professional services, transport, and telecommunications.

2. Key recommendations

The Business Council of Australia recommends:

1. The Bill be subject to a comprehensive assessment, including a full Regulatory Impact Statement.
2. The Committee ask Government to undertake an urgent review of the various laws and regulations that require (either directly or indirectly) businesses to collect and hold information about Australians.
3. Section 80U(1) provide for 'tiering' of penalties, and also explicitly set out that in determining penalties, courts be required to consider whether an organisation can show they were not negligent or reckless. This could be demonstrated through, for example, compliance with leading cybersecurity practices, development and implementation of frameworks providing appropriate governance and guidance for the ethical use of data, training programmes for team members and third parties servicing a business and robust privacy frameworks including policies. This should also include greater clarity and refreshed guidance on what constitutes a 'serious' or 'repeated' breach.
4. The Committee recommend government work with businesses to streamline the reporting requirements for privacy and cybersecurity breaches, to ensure the focus remains on protecting Australian citizens, not navigating bureaucracy and mitigating the potential liability issues for government.
5. Section 33B(1) should be reconsidered, or at minimum be amended to exceptional circumstances and require the OAIC to consult with affected entities ahead of disclosing any information, and to consider the proportionality of any information released. The types and nature of the information the Commissioner can release should also be further prescribed to reflect the policy intent of this section of the bill.
6. If an entity is responding to an actual or suspected breach, then the Information Commissioner should not be entitled to exercise the new information request powers until after a 30-day assessment period has passed from when the Information Commissioner was first made aware of the actual or suspected breach
7. The Bill be amended to clarify the extent of the extraterritoriality provisions, particularly so it does not extend to the regulation of information with no direct connection to Australia or potentially put Australian laws in direct conflict with laws in other jurisdictions.
8. Retrospectivity of specific schedules apply for a specific time period (eg six months before commencement), rather than for an unlimited duration.
9. The Committee recommend government designate a single adviser and coordinator with appropriate expertise to manage the government's response to these types of incidents.
10. The Committee recommend government continue to prioritise measures that improve Australia's overall cybersecurity and privacy, including addressing cyber security skills challenges and progressing the option of digital identity to allow for data minimisation across the public and private sector.

3. Overview

Businesses take seriously the obligation to protect Australian's personal information. As we have previously highlighted, cybersecurity is front of mind for CEOs in Australia, well ahead of other key risks, including economic volatility, health, climate change, or geopolitical conflict.[1]

But all Australian organisations – businesses, community groups, government agencies, political parties – operate in an increasingly challenging environment, as highlighted in the government's Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report.[2]

Cyber incidents are an inevitability for government, businesses, and individuals. It will be impossible to prevent all attacks. All frameworks put in place to respond to cyber incidents must recognise this. New attack methods, the discovery of zero-day vulnerabilities, leaking of government cyberattack tools, and sophisticated attackers all make it impossible for businesses to be immune to cyber incidents.

This is not to say businesses are passive victims. Businesses want to work in partnership with government on this threat.

This is why we need frameworks that enable businesses to invest in robust defences, and, where these may be defeated, early detection and investigation. When breaches occur, organisations need appropriate support from government agencies to enable the investigation to proceed swiftly, in a coordinated manner with minimum bureaucracy, delay and with the necessary support and resources from leading expertise and agencies such as the ASCS.

It is critical to have a regulatory regime that encourages the right behaviour. The blanket application of penalties to those suffering from the consequences of cybercrimes serves to increase the scale of harm for victims.

Fundamentally, all organisations need to continually be lifting their cybersecurity posture to match ever increasing and complex attacks. This needs to be done in partnership with government.

To achieve this, Australia needs to address the critical cybersecurity skills shortages. These are the most in-demand digital profession in Australia.[3] Without addressing skills shortages, all organisations will not be able to upgrade and maintain the appropriate controls necessary to protect themselves and information about Australians. There will be no one able to deliver on the intentions of the Bill.

This is not just about cyberattacks

The Committee must also recognise this legislation has wider implications than just responding to the recent spate of cyberattacks. The revised penalties will apply to the range of relevant offences under the Act, and potentially to any new provisions legislated as part of the Privacy Act Review.

This means the Bill must be considered within the context of the entire Act and – given the Act's reach – across all the economy and society.

The government's Australian Data Strategy highlights that data will be the 'lifeblood of our digital economy'.[4] The Productivity Commission has also highlighted the importance of the use of data to lift Australia's productivity.[5]

Australia's economic prosperity will hinge on our ability to develop, adopt, and use new technologies. Innovation driven by the lawful and ethical use of data will be fundamental to our prosperity and the prosperity of future generations. The importance of data to deliver good outcomes for Australians has been recognised not only by

[1] https://www.pwc.com.au/ceo-agenda/ceo-survey/pwc-australia-25-ceo-survey.pdf. Note this survey was conducted well ahead of the recent cybersecurity incidents.
[2] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022
[3] https://www.nationalskillscommission.gov.au/reports/digital-skills-australian-and-international-economies
[4] https://ausdatastrategy.pmc.gov.au/
[5] https://www.pc.gov.au/inquiries/current/productivity/interim2-data-digital/productivity-interim2-data-digital.pdf

businesses, but also by key government agencies like the Department of the Prime Minister and Cabinet, the Treasury portfolio, the Australian Bureau of Statistics, and many others.

Disproportionate or unnecessary penalties and haphazard enforcement powers will increase the hurdles for all organisations looking to deliver better products and services to Australians. Worse, it will undercut the ability for all sectors to deliver better, high paying jobs.

It is unlikely to be large businesses that will be most seriously punished. It is the smaller businesses and entrepreneurs looking to create good jobs for Australians that these types of laws will most negatively affect. Even if the maximum penalties are not pursued for these group, they still send a negative signal about Australia's attitude towards innovation and the use of data. Those with new ideas will go offshore to start their businesses.

For this reason, not only should penalties be set in a proportionate way, but appropriate guardrails must be put in place. Businesses of all sizes understand the need to take this seriously, and these increased penalties reinforce this point. But the Privacy Act must still support businesses that innovate through the appropriate use of data.

4. Key points

The Bill's quick introduction and short consultation period has meant businesses have not been adequately consulted on the changes. It is also coming ahead of the comprehensive reforms through the Privacy Act Review. This increases the risk of mistakes, unintended consequences, and may undermine delivering on the policy intent.

The changes outlined in the Bill seek to "enhance the protection of personal information". However, it is unclear how the significantly increased penalties, enabling regulators to demand more information, and allowing bureaucrats to speak to each other will lift the levels of privacy protections for Australians. Better privacy outcomes need to be delivered through the comprehensive review of the Privacy Act, to ensure a coherent, consistent, and system-wide approach is delivered.

Moreover, increasing penalties in isolation without amendments to the Privacy Act as a whole does not assist business in lifting compliance, but merely increases the risk to the business. Similarly, changing enforcement and information sharing regimes ahead of potentially significant changes to the overall Act may create substantial unintended consequences. It would be worthwhile considering whether components of the Bill unrelated to penalties should be split out, for more sober consideration as part of the overall Review.

The Bill should be subject to a comprehensive assessment with adequate consultation that considers all options to "enhance the protection of personal information", including a Regulatory Impact Statement.

Further, some changes proposed through this Bill (such as the information sharing powers) were suggested by the previous government through the Online Privacy Bill. Our responses to these changes have not changed, and it is concerning that in preparing this Bill the problems we highlighted with the previous Bill have not been addressed, such as with the new powers allowing the OAIC to unilaterally publish information collected in its investigation.

4.1 Business data collection

Underpinning much of the discussion on the recent cyberattacks has been the assertion that businesses collect and hoard personal information haphazardly and for selfish commercial pursuits that come at the expense of Australians.

This is an inaccurate generalisation about the data landscape in Australia.

Businesses, like government, collect and use data to deliver not just better but also basic and essential services and experiences for all Australians. In responding to health needs, data obtained from individuals is used to provide care and treatment to them. But it can also be used in a de-identified form (as per the government's

Australian Privacy Principles) to better understand how different populations respond to healthcare treatments and to inform the development and creation of new healthcare interventions that improve patient outcomes. Indeed, the independent review into Australia's response to COVID-19 highlighted the importance of data sharing to Australia's management of the pandemic.[6]

This is not to excuse the holding of data longer than needed or required by the law. Nor is it to diminish or defray responsibility or accountability. But it would be overly simplistic to assert that businesses should (or can) simply delete all data immediately.

Businesses are compelled to collect information by the government through a range of legislation and regulation that has built up over many years.

This can include the collection of information to prevent criminals and organised crime from stealing Australian's phone numbers (SIM swapping), preventing money laundering or financing of terrorist groups (such as Know Your Customer requirements imposed on financial institutions), to comply with requirements imposed by the Australian Taxation Office to support revenue collection, for intelligence purposes (such as metadata retention), or to potentially respond to court orders.

Successive governments have also been encouraging businesses to use and share data, including through initiatives like the Consumer Data Right. Government itself has sought to make data sharing easier for itself, including through the Data Availability and Transparency Act, which passed with bipartisan support in the last Parliament.

Many organisations, including the BCA and many businesses, have long argued that government should pursue reforms that bring the priorities of these various pieces of work into alignment, and harmonise the various regimes governing the use of data in Australia.

Despite this, further reforms requiring greater collection of personal information have also been broached, including as part of online safety regimes and electronic surveillance reforms.

Existing laws are opaque about whether businesses are required to hold the data necessary to fulfill their obligations. Realistically, to be able to demonstrate compliance and support government priorities, businesses must retain this information.

> Telecommunications (Interception and Access) Act 1979 and the Telecommunications Act 1997
>
> Complex requirements under the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979* require telecommunications providers to hold a complex array of different types of personal information for differing periods of time and for different purposes, including law enforcement activities and the prevention of crime.
>
> For example, if ID documents are obtained to identify a customer, a telecommunications provider is required to retain ID information for two years post-closure of a customer account.
>
> Anti-Money Laundering and Counter-Terrorism Financing Act 2006
>
> To prevent financial crimes and financing of terrorists, the Act requires customer verification records and identification records to be kept by financial services providers and other 'reporting entities' for 7 years after the last interaction/service was provided to that customer.
>
> This is far beyond the time financial institutions want or need to hold customer information. It exposes these organisations to greater risk in the event of any cyber incident

What is needed is clarity from government about its expectations for the regulatory requirements to collect and hold information about Australians. Many of these laws have been in place for decades, often without review or

[6] https://www.paulramsayfoundation.org.au/news-resources/fault-lines-an-independent-review-into-australias-response-to-covid-19

modernisation to reflect new technologies. The complex web of data retention laws have been put in place by both the Commonwealth and state and territory governments, and apply across different sectors in Australia. They require certain information to be kept for 2 years, 5 years, 7 years and even 10 years in some cases. Consequently, there is a tendency for regulated entities to keep personal and other information for the longest prescribed period to ensure they meet legislative requirements.

We recommend the Committee ask Government to undertake an urgent review of the various laws to provide businesses with the clarity they need and to then enable business to act on removing data no longer legally required.

4.2 Increased penalties

The Attorney-General has announced his intention through this Bill to increase these penalties for serious or repeated interferences with privacy to align with the proposed competition penalties (a maximum of the greater of $50 million, three times the benefit received, or 30 per cent of turnover for the relevant period). The current maximum penalty under privacy laws is $2.22 million for serious breaches of privacy. The Privacy Act covers companies with annual turnover above $3 million (though excludes registered political parties).

If applied to a large business, the maximum would exceed by several multitudes the existing highest corporate penalty applied in Australia. The size of these penalties, if applied to their maximum extent, could result in a business becoming bankrupt, particularly smaller businesses.

These penalties are being introduced in the context of cyberattacks affecting organisations across Australia. But for cyberattacks, the logic of deriving penalties through looking at 'benefits' (or, where these can't be determined, turnover) is nonsensical. The 'benefits' an entity derives from being the victim of crime can only be measured in the negatives – through lost reputation, customers, revenue, intellectual property, or other assets, and the costs of remediating and mitigating the fallout.

Moreover, as stated above, cyber incidents are impossible to fully prevent. Organisations (businesses, government agencies, political parties, and community groups) may become a victim because of previously unknown vulnerabilities (zero-days) or highly sophisticated state, criminal or other actors. It is unreasonable to expect organisations to be able to protect themselves against all of these kinds of attacks every single time. The ACSC has acknowledged the difficulty of defending against these kinds of attacks and previously noted the increasing trend towards criminal and state actors rapidly taking advantage of these vulnerabilities.[7]

In this context, any policy framework and response must clearly differentiate between incidents which occur due to negligent or reckless failure by an entity to take reasonable steps and those where the entity is a victim of sophisticated, targeted, and unprecedented actions by criminal and/or state actors. Duties of entities in this area and the consequences of a breach must be appropriate and proportionate to the actual wrongdoing or failure by the entity and the damage resulting to the entity, its employees, customers, and other stakeholders.

Cybercrime is evolving and by nature adversarial. It is not realistic to expect that data breaches will cease due to businesses being able to obtain a level of security which is incapable of breach. Criminal attacks will continue to happen, and some will be successful as new weaknesses are uncovered.

We already know criminals calibrate their demands according to the insurance taken out by businesses. Criminals will demand ransoms proportionate to the potential penalties – higher penalties will mean higher ransom demands.

In the face of sophisticated state actors, businesses are at an even greater disadvantage.

This is why that as we acknowledge the intent to increase penalties, they should be proportionate and not impose undue hardship on businesses that are taking responsible steps to protect personal information. Penalty regimes should not punish victims and instead be directed at those who have acted or failed to act in

[7] *ACSC Annual Cyber Threat Report, July 2020 to June 2021.*

circumstances which indicate they were negligent and/or reckless or failed to comply with laws which would have prevented the breach had they complied.

The penalties this Bill will introduce will apply to breaches of the Privacy Act, including changes that are yet to be introduced or even publicly discussed through the Privacy Act Review. It is impossible to assess the appropriateness or proportionality of the penalties proposed in the Bill until the further reforms have been proposed and understood.

Unlike penalties under competition law, there is little to no jurisprudence or prior cases to draw on in contemplating penalties under the Privacy Act.

For this reason, we recommend the Bill be amended to provide greater guidance and 'tiering' for penalties.

This would retain the spirit of the existing Act, and mirror the penalty regime under the GDPR, which specifies a scaled approach to setting and capping maximum penalties that are proportionate to the seriousness and frequency of various breaches of the law.

It would also be aligned with the proposals put forward in the Discussion Paper released by the Attorney-General's Department as part of the Privacy Act Review. Proposal 24.1 in the Discussion Paper suggested creating tiers of civil penalties to give the regulator more options to better target regulatory responses. This included:

- A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.
- A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.

Greater clarify should also be provided through defining 'serious and repeated' under section 13G of the Privacy Act, as was set out under Proposal 24.2 of the Privacy Act Review Discussion Paper.

Alternatively, it could be incorporated within section 80U of the Privacy Act. This section of the Act currently sets out that in determining pecuniary penalties a court must take all relevant matters into account. These include the circumstances of the contravention, the nature and extent of any loss or damage suffered because of the contravention and whether the entity has previously been found to have engaged in similar conduct.

Part 4 of the Regulatory Powers (Standard Provisions) Act 2014 requires courts to take several matters into consideration when determining a penalty. The Act sets out that the court must consider:

a) the nature and extent of the contravention; and

b) the nature and extent of any loss or damage suffered because of the contravention; and

c) the circumstances in which the contravention took place; and

d) whether the person has previously been found by a court (including a court in a foreign country) to have engaged in any similar conduct.

These provisions are very strong, and in combination with section 80U of the Act, ensure a court is able to take into consideration the negative effects (eg the nature and extent of any loss or damage suffered because of a privacy breach). But as discussed above, privacy breaches resulting from cyber incidents are impossible to fully prevent. Point C of the Regulatory Powers Act referred above also needs to provide positive incentives for businesses to invest in appropriate security and controls.

To ensure all organisations are incentivised to take the right security steps, the Bill should amend Section 80U(1) to provide clarity on what 'circumstances' a court should consider. These should include:

- Whether a breach was the result of deliberate, reckless, or negligent behaviour on the part of the regulated entity,
- Whether a regulated entity was compliant with recognised or prevailing standards for security and had robust privacy frameworks in place,

- Whether an entity acted promptly to investigate the matter, sought appropriate expert assistance, and worked in good faith to address harms to citizens, and
- Whether an entity disclosed the breach at an appropriate time to mitigate damage to all involved.

As noted above, this requires revised guidance from the relevant regulator (the OAIC) on how a 'serious' breach will be determined. Current guidance from the OAIC is too broad and punitive in that it fails to recognise the various circumstances that can lead to a privacy breach and therefore effectively supports an approach that potentially punishes wrongdoer and victim alike. It also needs to include guidance on how a 'period of contravention' will be calculated when defining a breach turnover period.

4.3 Reporting and a coordinated government response

The committee should also recommend government work with businesses to streamline the reporting requirements for privacy and cybersecurity breaches.

All organisations, including businesses, need to operate in an environment that encourages disclosure as soon as practical. It is only through partnerships between businesses, government, and the community that Australia will build and maintain cyber resilience. A coordinated approach by government and businesses to notification of authorities, expert investigation, and urgent dedication of skilled resources the only way Australian citizens, government and businesses can work together to mitigate the risks and far-reaching harms of cybercrime.

There is already a 'forest' of reporting requirements businesses and other organisations must comply with, each with varying timeframes and requirements. Simplification is going to be critical. Government must adopt a coordinated response when these incidents occur.

This will not be easy, but it is essential. It will mean looking at reporting requirements under a wide range of bodies, including under the critical infrastructure act, APRA requirements, the Notifiable Data Breaches Scheme, among a raft of others. And it will mean looking at how government can better set itself up to respond to future attacks. This is vital: in the event of an attack or privacy breach, a business should not be focusing on discharging reporting requirements and navigating red tape, but instead at remediation and protection of citizens.

A single adviser and coordinator must be designated to bring together the various arms of government requests, responses and issue detailed advice – similar in some ways to the role of the Chief Health Officer during COVID. This role – which would fulfil a role like a CIO for government – could assist in building public confidence in the response.

4.4 Extraterritoriality

The Bill will also amend the extraterritorial jurisdiction of the Privacy Act. This is intended to ensure foreign organisations who carry on business in Australia must meet the obligations under the Act, regardless of whether they collect or hold information even in relation to personal information that they collect from individuals who are not in Australia.

The current drafting means that if a US based corporation provides services to Australians, the new drafting will mean that the Privacy Act would also apply to that corporation's handling of information about users in the US or in any other jurisdiction where that corporation makes its services available.

It is unclear why the Australian Parliament would seek to regulate the management of personal information where there is no connection to Australia. It also risks bringing Australian laws into conflict with requirements made in other jurisdictions.

Given there isn't a clear justification for this, it appears this is an unintended drafting error. We recommend this be amended before the Bill receives passage.

4.5 Information gathering powers

The OAIC will be granted new powers to gather information in response to an actual or suspected notifiable data breach. This must be bounded by some form of time-based requirement.

If an entity is responding to an actual or suspected breach, then the Information Commissioner should not be entitled to exercise those powers until after a 30-day assessment period has passed from when the Information Commissioner was first made aware of the actual or suspected breach. Businesses may not have notified Commissioner as they actively investigate and determine the extent of the breach. Information requests at this time may well be at best a distraction and at worst actually cause the relevant entity to take its focus away from the main objective of securing the breach and protecting data subjects.

It is important to ensure that disclosure is well managed and avoids confusion or misinformation. Any regime that is intended to cause early disclosure should be carefully considered when compared with the harm that may occur either to stakeholders as a result, or to the effective investigation into or remediation of the breach itself.

4.6 Publication of information by regulators

The Bill is intended to enhance the OAIC's enforcement powers. The new clause 33B(1) enables the OAIC to disclose publicly, information acquired during an investigation if it believes this is in the public interest and may even disclose such information before the investigation is complete. This is completely contrary to how the OAIC currently conducts investigations and contrary to how most regulators conduct their investigations. The rationale given in the Explanatory Memorandum for this section was "***to reassure the community that the OAIC is discharging its duties***". This is not an appropriate reason for disclosure of information in these circumstances.

We have previously objected to this type of blanket power. As we set out in our submission on the Online Privacy Code, where this was originally proposed, there is no limitation as to the nature of information that may be disclosed. Accordingly, disclosed information might include any information supplied to the Commissioner in the course of an investigation, regardless of whether that information is contested as to accuracy, completeness or relevance.

There is no requirement of prior consultation with the person or entity that provides the relevant information or to whom the information relates. There is also no requirement for the Commissioner to consider proportionality or to balance benefit to the person or entity that provide the relevant information or to whom the information relates against, merely to "have regard" to the matters specified in proposed section 33B(2).

This could lead to situations where the OAIC publishes information that will allow further attacks to be made against an organisation, if the OAIC fails to understand the nature of the information it is releasing. Moreover, disclosing during an investigation information obtained as part of the investigation has the potential to undermine, compromise and delay any such investigation. Rather than investigating the incident and cooperating with the OAIC, the company may end up spending most of its time dealing with the unintended consequences of a premature public disclosure if selective information is disclosed in this way.

There may be exceptional circumstances where due to an emergency or the company's limitations it is necessary for the OAIC to make such a disclosure, but this should be an exception, not the rule, and the proposed provision should reflect this rarity and contain safeguards. Otherwise, this may discourage companies from disclosing matters to the OAIC, as they may perceive this will make the investigation process more complex and difficult.

The government should also consider placing greater checks and balances to this power. At a minimum, section 33B(1) should be amended to require the OAIC to consult with affected entities ahead of disclosing any information, and to consider the proportionality of any information released. This includes through incorporating an express requirement to consider the potential risks to the effective investigation and remediation of the breach itself and the risk of harm to the entity, other entities in Australia and national security before any disclosure is made.

The types and nature of the information the Commissioner can release should also be further prescribed to reflect the policy intent of this section of the bill.

Further, the introduction of a new criminal offence in s.66(1AA) where a system of conduct or a pattern of behaviour results in two or more breaches of the requirement on companies to answer questions or produce documents, appears a disproportionate response to a problem that does not appear to exist. It is suggested that serious consideration be given to whether this provision is warranted.

4.7 Sharing of information acquired through investigations

The Bill provides the OAIC and ACMA with greater information sharing powers. This will allow the sharing of information with an enforcement body, alternative complaint body, State or Territory authority or an authority of a foreign government that has privacy functions.

While we understand the need for relevant government bodies to regulate and respond to data breaches, the proposed expansion of information-sharing powers is broad and may have unintended implications for Australians.

When sharing information acquired through investigations or provided confidentially and in good faith by a business, to ensure integrity in government, governance needs to be in place.

We recommend that, at a minimum, the information sharing powers be amended to require the OAIC to inform the relevant organisation that both the sharing is occurring and for what purpose. This will allow the organisation to provide additional or supporting context to the receiving agency, if needed.

Haphazard sharing of information by the regulator (or publication, as discussed above) may have substantial adverse consequences, including distracting an organisation from remediating the breach and protecting any affected individuals.

The proposed information sharing powers could also create a double jeopardy risk for entities where information is shared between regulators under broadly defined powers. In addition, we are concerned that information gained in one context, when provided to another agency for an associated but perhaps different context, may be incorrectly relied upon.

Further, the threshold for sharing information is too low, and does not provide adequate safeguards to protect the information or documents shared with other authorities. The current test ('the Commissioner is satisfied on reasonable grounds that the receiving body has satisfactory arrangements in place for protecting the information or documents') must be strengthened. The term 'satisfactory arrangements' is broad and potentially subjective and not in the interest of protecting personal information, or commercially sensitive information of the impacted organisation or business.

The proposal to amend section 59D of the ACMA Act to expand ACMA's ability to share information with 'any non-corporate Commonwealth entity responsible for enforcing a Commonwealth law where the information will enable or assist the entity to perform or exercise any of its functions or powers' is also quite broad and could exacerbate the above risks.

Without this, a Bill ostensibly intended to enhance Australian's privacy and prevent unauthorised transfers will instead create the perverse situation where private and confidential information will be allowed to wash throughout government and to foreign governments with little to no controls or governance.

4.8 Retrospectivity

Through proposed section 45, the Bill allows retrospective application for some of the new powers, including the OAIC and ACMA's ability to disclose information (under proposed sections 33A and 33B, and subsection 59D(1) of the *Australian Communications and Media Authority Act 2005*).

It is not clear why uncapped retrospective application of these new powers is necessary. While we believe this is likely to enable the OAIC and ACMA to share information about the recent attacks on businesses, this is not set out anywhere.

Unless a clear explanation for this can be given, it would seem prudent to provide greater certainty about how far back these powers can extend. We recommend that rather than specifying that the schedules apply 'before or after' commencement, the Bill instead provide that the schedules apply for a specific period (eg six months before commencement).

4.9 Protecting Australian's data

We also acknowledge that our recommendations are only part of the solution to tackling cybercrime and supporting businesses to handle information about Australians appropriately. Businesses and government agencies need to take steps to lift their own security, including through putting in place both appropriate technical controls as well as high quality process and business practices (such as regular training and testing).

We welcome the cooperation businesses have had with government on continued efforts to uplift cybersecurity across Australia, through the Essential Eight program and related activities by various departments including Home Affairs, the ACSC and the ASD.

The Committee should recommend government continue to prioritise addressing these skills challenges and progressing digital identity.

Important government initiatives like the digital identity framework need to be progressed and provide businesses with an alternative voluntary option to physical credentials to verify Australian's identities. Australians have little choice but to use documents like passports and driver's licences as accreditation. Much like the US's Social Security Number, these are difficult to revoke and replace. This is particularly important for smaller organisations, where it will be not possible for them to minimise the data they need to collect or hold without appropriate resourcing.

As noted at the start of this submission, Australia needs to address the critical cybersecurity skills shortages. This will be the only way government, businesses, and the community can meet the cybersecurity challenge all Australia faces. The other focus should be on ensuring there are appropriate laws and legal resources dedicated to addressing cybercrime. Punishing the victim of cybercrime does not help prevent the crime itself.

As part of the forthcoming consultation on the refreshed Cyber Security Strategy, the government also needs to work with businesses on other key initiatives, including through:

- tax incentives to invest in cybersecurity tools and training for businesses,
- accelerated amortisation schedules for IT transformation projects,
- investment in education and upskilling of the population,
- supporting public-private partnerships and the innovation ecosystem to ensure solutions are keeping pace with the threat landscape, and
- encouraging and supporting threat intelligence sharing across business sectors with respective government agencies and suppliers to work together to mitigate the risks.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au